



GPON ONT PMG5318-B20B

Application Note

version 1.0

March 2016

Contents

Getting to Know the Device	1
Integrated Internet Services Through Fiber Optics	1
2.4 GHz 11n (2x2) for superior performance and coverage	1
Advanced Quality of Service ensures quality of triple-play services.....	1
Provisioning and management through TR-069 along with OMCI.....	2
General Application Diagram	2
General Scenario 1: Internet Service Only.....	2
Example Devices	3
Switch Setup	3
OLT2406 Initial Setup.....	6
OLT2406 CLI Setup	10
Adding a new PMG5318-B20B	10
Checking the ONT status.....	11
ONT Web GUI Setup	13
General Scenario 2: Triple Play	20
Example Devices	20
Switch Setup	20
OLT2406 CLI Setup	23
Adding a new PMG5318-B20B	24
Checking the ONT status.....	25
ONT Web GUI Setup	27
Data Service Setup.....	29
VoIP Service Setup	34
IPTV Service Setup	40
Test IPTV Bridge using VLC.....	43
Frequently Asked Questions	50

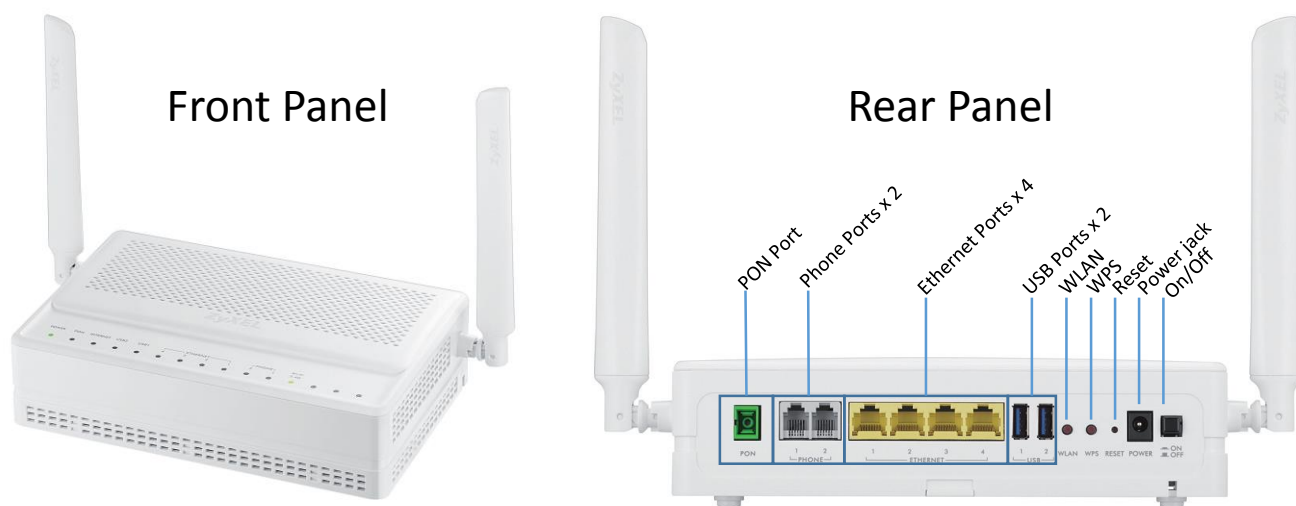
General Questions	50
Device Info Tab	51
Hardware.....	51
Summary	53
WAN	56
Statistics	56
Route	57
ARP	58
DHCP.....	59
Advanced Setup Tab	60
Layer 2 Interface	60
WAN Service	60
NAT.....	60
Security.....	61
Parental Control.....	62
Routing	63
DNS.....	65
Storage Service	67
Remote Management.....	68
Wireless Tab	68
Diagnostics Tab.....	73
Management Tab.....	75

Revision History

Date	Release	Author	Description
2016/03/04	1.0	Emanuel Villalobos	First draft, proofread by Henry Chang and Claire Lai

Getting to Know the Device

PMG5318-B20B is a GPON ONT that provides high-speed fiber access combines with residential gateway, VoIP and wireless features. It is compatible for optical ITU-T G.984 and wireless IEEE 802.11n environment.



Integrated Internet Services Through Fiber Optics

The ZyXEL PMG5318-B20B Wireless N GPON HGU with a 4-port GbE Switch provides various integrated services through a single optical fiber for customers to support prevalent deployments of triple-play services such as data, video/high-definition television (HDTV), VoIP and interactive games.

2.4 GHz 11n (2x2) for superior performance and coverage

The ZyXEL PMG5318-B20B features 802.11n technology to provide an ultimate solution for both speed and coverage. With 802.11n wireless data rates of up to 300 Mbps, the PMG5318-B20B provides stable, reliable wireless connections for high-speed data and multimedia applications. The 802.11n technology empowers the device to eliminate dead zones and to extend coverage while retaining backward compatibility with any IEEE 802.11 b/g/n Wi-Fi certified device.

Advanced Quality of Service ensures quality of triple-play services

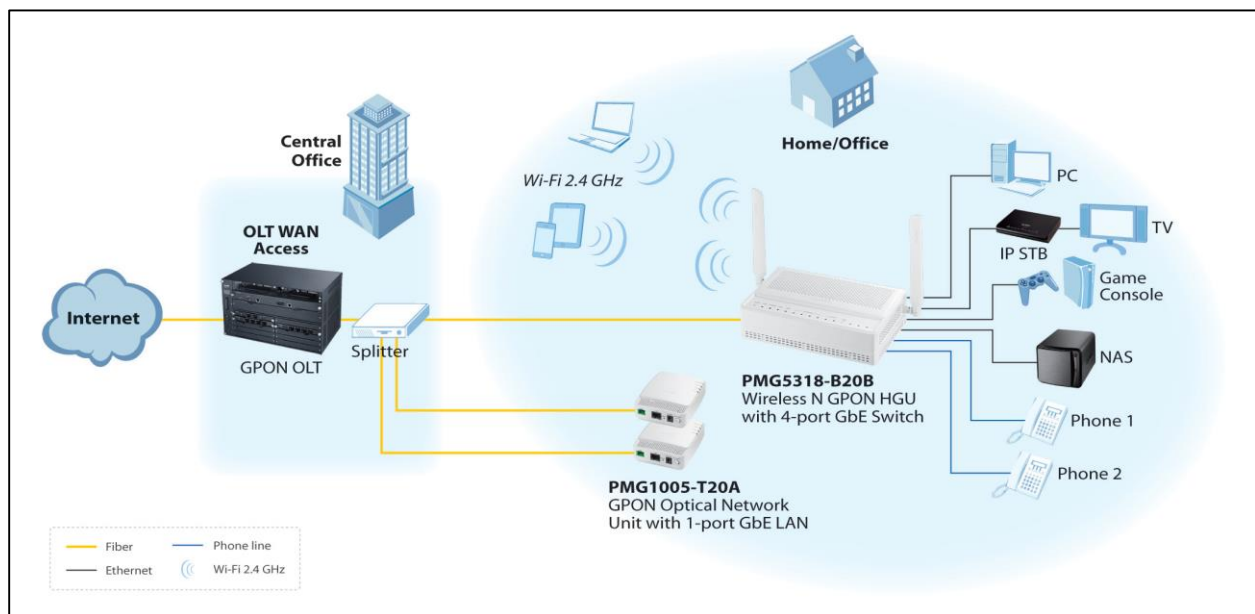
As higher bandwidth and greater efficiency of Ethernet cannot ensure effective delivery of high-quality voice, data and video across a GPON network, service

providers can freely design their Quality of Service (QoS) policies and prioritize mission-critical services such as IPTV and VoIP based on their service plan offerings. This increases network efficiency and productivity to enable service providers to offer a real multi-play solution that meets the needs of residential users.

Provisioning and management through TR-069 along with OMCI

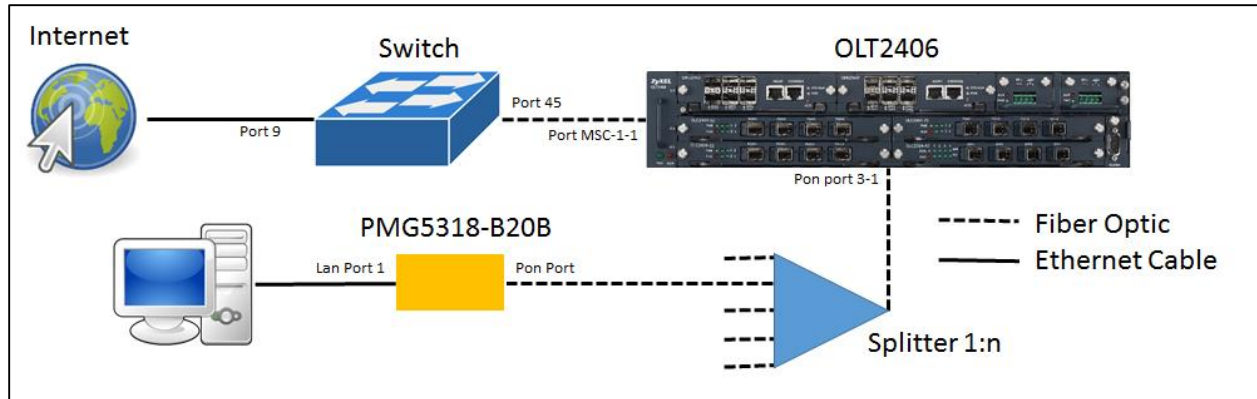
The ZyXEL PMG5318-B20B can be connected to a GPON OLT to provide network operators with management and provision functions that support ONT Management and Control Interface (OMCI) as well as TR-069 management functions. As a result, the operation and maintenance of the PMG5318-B20B are extremely easy and efficient.

General Application Diagram



General Scenario 1: Internet Service Only

In this scenario we will configure ZyXEL’s Switch, OLT and ONT for Internet service only using VLAN 100 as an example.



Example Devices

- A. OLT: OLT2406, FW: 4.00(AAVA.4)C0
- B. ONT: PMG5318-B20B, FW: 100AAZC0C0
- C. Switch: GS2200-48

Switch Setup

Switch web GUI > Advanced Application > VLAN > Static VLAN

1. Check Active Box.
2. Set the name for the VLAN.
3. Set the VLAN Group ID. (VLAN ID).
4. Select the ports to be members of this VLAN as Fixed, and select the port to be Tagged or Untagged.
5. Click the "Add" button at the end of the page to save your changes.

Static VLAN VLAN Status

1 ACTIVE

2 Name Data

3 VLAN Group ID 100

Port	Control			Tagging	
*	Normal			<input checked="" type="checkbox"/> Tx Tagging	
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
7	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
8	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
4	9	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging	
44	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
5	45	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
46	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
47	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
48	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
49	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	
50	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging	

5 Add Cancel Clear

In this example, switch port 9 and 10 will be used for access traffic (to internet), and port 45 will be used for the tagged traffic (to the OLT) using VLAN 100.

It is possible to check the current status of the VLAN by accessing:

Switch web GUI > Advanced Application > VLAN

Then proceed to click the index number for the VLAN ID you wish to verify.

VLAN Status		VLAN Port Setting		Static VLAN	
The Number of VLAN = 3					
Index	VID	Elapsed Time	Status		
1	1	94:43:49	Static		
2	100	94:38:49	Static		
3	2302	94:39:25	Static		

A new page will show containing the port diagram and the status of each port where “U” is untagged and “T” is tagged.

VLAN Detail		VLAN Status																									
VID	Port Number																			Elapsed Time	Status						
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38			40	42	44	46	48	50
100	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	T	-	-	94:42:33	Static

For the untagged ports, then proceed to add a PVID at the following location:

Switch web GUI > Advanced Application > VLAN > VLAN Port Settings

Set the PVID according to the VLAN membership:

VLAN Port Setting		Subnet Based Vlan		Protocol Based Vlan		VLAN Status	
GVRP		<input type="checkbox"/>					
Port isolation		<input type="checkbox"/>					
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking		
*	<input type="checkbox"/>		<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
9	<input type="checkbox"/>	100	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
10	<input type="checkbox"/>	100	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>		

Ports 9 and 10 being untagged, proceed to setup the PVID to 100. For port 45 no PVID is required as it will be passing tagged traffic.

OLT2406 Initial Setup

How to read this section, in gray boxes you will find the executable CLI commands, meanwhile in yellow screenshots you'll find the input of commands for example cases.

To set the OLT for first use, start by activating the Slots:

```
Configure
Interface slot slot-3
Cardtype gpon
No inactive
exit
```

```
OLT2406# configure
OLT2406(config)# interface slot slot-3
OLT2406(config-slot)# cardtype gpon
OLT2406(config-slot)# no inactive
OLT2406(config-slot)# exit
```

To verify the Slot configuration, use the following commands:

```
Show lc status
```

```
OLT2406# show lc status
48V power: Input-A up, Input-B down
Slot Id      State      Card Type      Up Time
-----
1            active     MSC            23:20:36
2            -         MSC            -
3            active     GPON           0:05:17
4            inactive
5            -
6            -
OLT2406#
```

```
Show interfaces slot slot-3 status
```

```

OLT2406# show interfaces slot slot-3 status
-----
AID          | Base_Address      IP0          IP1          MAC0          MAC1 Support_Link
-----
slot-3      | 0x be000000      127.168.0.1 127.168.0.2 00:a0:c5:00:00:07 00:a0:c5:00:00:08 0
-----
| Details
-----
| Status: READY
| Device Version: 0x2060701
| Driver Version: 0
| Firmware Date: Dec 25 2012, 17:50:33
-----
OLT2406#
    
```

After activating the slots, it is now possible to enable the PON Interface:

```

Configure
Interface olt pon-3-1
Transceiver 12
Register method A
No inactive
exit
    
```

```

OLT2406# configure
OLT2406(config)# interface olt pon-3-1
OLT2406(config-olt)# transceiver 12
OLT2406(config-olt)# register-method A
OLT2406(config-olt)# no inactive
OLT2406(config-olt)# exit
OLT2406(config)#
    
```

The Registration methods are defined per the following table:

Registration Method	Definition
A	Require Serial Number and Password.
C	Requires the Password.
C-Autolock	Requires the Serial Number.
D	Automatically registers the ONT and brings it into service without checking the serial number or password. <u>The ONT may receive a different ONT ID when it reconnects.</u>

E Automatically registers the ONT and brings it into service without checking the serial number or password. The OLT records the SN/ONT ID mapping and uses the same ONT ID for the ONT when it reconnects.

And the Transceiver available are referenced as follow:

```

OLT2406(config-olt)# transceiver 99
Transceiver type

LIGENT           = 0
LUMINENT         = 1
FIBERXON        = 2
FUJITSU         = 3
LIGENT_A        = 4
LIGENT_B        = 5
LIGENT_C        = 12
LUMINENT_A      = 6
LUMINENT_B      = 7
FIBERXON_A     = 8
FIBERXON_B     = 13
FUJITSU_A      = 9
NEC             = 10
NEOPTec        = 11
FUJITSU_30537  = 14
NEOPHOTONICS_A = 15
NEOPHOTONICS_B = 16
NEOPHOTONICS_C = 17
SUPERXON       = 18
WTD            = 19
DELTA          = 20
1              = 21
2              = 22

OLT2406(config-olt)# transceiver ?
<type>          transceiver type 0~22
tx-disable      Tx Disable
    
```

To display the list write a transceiver number out of range

For ZyXEL's OLT Always select type 12

To create an ingress profile, execute the following commands:

```

Configure
qos ingprof alltc0 dot1p0tc 0 dot1p1tc 0 dot1p2tc 0 dot1p3tc 0 dot1p4tc 0 dot1p5tc 0 dot1p6tc 0 dot1p7tc 0
    
```

```

OLT2406# configure
OLT2406(config)# qos ingprof alltc0 dot1p0tc 0 dot1p1tc 0 dot1p2tc 0 dot1p3tc 0 dot1p4tc 0 dot1p5tc 0 dot1p6tc 0 dot1p7tc 0
    
```

The QoS Bandwidth profile will be setup as:

```

Configure
qos bwprof 10M sir 1024 air 5120 pir 10240
    
```

Additional help on setting the bandwidth profile can be viewed using the help command as follow:

```

OLT2406# configure
OLT2406(config)# qos bwprof help
  Commands available:

  qos Bwprof <name>
  <
    [ sir <0-2400000> ]
    [ air <0-2400000> ]
    [ pir <0-2400000> ]
  >
  example cmd: qos Bwprof test  sir 1024 air 2048 pir 5120
  The value of sir/air/pir will be rounded up or down to nearest multiple of 64 kbps.
  US TCONT Type
  +-----+-----+-----+-----+-----+
  |  Type1  |  Type2  |  Type3  |  Type4  |  Type5  |
  +-----+-----+-----+-----+-----+
  |   sir   |         |         |         |   sir   |
  +-----+-----+-----+-----+-----+
  |         |   air   |   air   |         |   air   |
  +-----+-----+-----+-----+-----+
  | pir=sir | pir=air | pir>air |  pir   | pir>=sir+air |
  +-----+-----+-----+-----+-----+
OLT2406(config)# qos bwprof 10M sir 0 air 0 pir 10240
OLT2406(config)#

```

Each VLAN can be setup using the following procedure:

```

configure
vlan 100
name data //optional: set a name for the vlan
fixed msc-1-1
fixed ge-3-1
no inactive
exit

```

```

OLT2406# configure
OLT2406(config)# vlan 100
OLT2406(config-vlan)# name data
OLT2406(config-vlan)# fixed msc-1-1
OLT2406(config-vlan)# fixed ge-3-1
OLT2406(config-vlan)# no inactive
OLT2406(config-vlan)# exit
OLT2406(config)# exit

```

OLT2406 CLI Setup

Adding a new PMG5318-B20B

To add a new ONT by CLI start by finding the Serial Number and Password after connecting the PON Port and turning on the device.

```
show remote ont unreg
```

```
OLT2406# show remote ont unreg
Pon_AID          |      Type          SN          Password          Status
-----+-----+-----+-----+-----
pon-3-1         |      UnReg 5A5958454150002E      1234567890      Active
-----+-----+-----+-----+-----
OLT2406#
```

Now proceed to create a new ONT ID with the specification for the new ONT. For this example, a QoS Bandwidth profile named 10M with SIR 1024, AIR 5120, and PIR 10240 Kbps will be employed.

```
configure
remote ont ont-<slot>-<port>-<ontID>
sn xxxxxxxxxxxxxxxx
pa xxxxxxxxxx
model 5
bwgroup 1 ustype 5 usbwprofname 10M dsbwprofname 10M
no inactive
exit
```

```
OLT2406# configure
OLT2406(config)# remote ont ont-3-1-1
OLT2406(config-ont)# sn 5A5958454150002E
OLT2406(config-ont)# pa 1234567890
OLT2406(config-ont)# model 5
OLT2406(config-ont)# bwgroup 1 ustype 5 usbwprofname 10M dsbwprofname 10M
OLT2406(config-ont)# no inactive
OLT2406(config-ont)# exit
```

After creating the ONT-ID we will proceed to setup the ONT card, for this we will select card 3 which corresponds to the managed entity for Router in the ONT, then we will define the type of card as VEIP (reference for router mode) and set the data ports as one.

```
remote ontcard ont-<slot>-<port>-<ontID>-3
cardtype VEIP data-port 1pa xxxxxxxxxx
no inactive
exit
```

```
OLT2406(config)# remote ontcard ontcard-3-1-1-3
OLT2406(config-ontcard)# cardtype VEIP data-port 1
OLT2406(config-ontcard)# no inactive
OLT2406(config-ontcard)# exit
```

After setting the router ONT card, we may activate the “ontvenet” as follow.

```
remote ontvenet ontvenet-<slot>-<port>-<ontID>-3-1
no inactive
exit
```

```
OLT2406(config)# remote ontvenet ontvenet-3-1-1-3-1
OLT2406(config-ontvenet)# no inactive
OLT2406(config-ontvenet)# exit
```

Finally, we will setup the UNI port queue and VLAN. For this example, a QoS ingress profile was defined with the name “alltc0” setting all priorities to traffic class 0.

```
remote uniport uniport-<slot>-<port>-<ontID>-3-1
queue tc 0 priority 0 weight 0 usbwprofname 10M dsbwprofname 10M dsoption olt bwsharegroupid 1
vlan 100 ing alltc0
exit
```

```
OLT2406(config)# remote uniport uniport-3-1-1-3-1
OLT2406(config-remote-uniport)# queue tc 0 priority 0 weight 0 usbwprofname 10M dsbwprofname 10M dsoption olt bwsharegroupid 1
OLT2406(config-remote-uniport)# vlan 100 ing alltc0
OLT2406(config-remote-uniport)# exit
```

Checking the ONT status

After completing the ONT setup, we can verify the status of it’s different elements.

```
Show remote ont ont-<slot>-<port>-<ontID>
```

```

OLT2406# sh remote ont ont-3-1-1
-----+-----+-----+-----+-----+-----+-----+-----+-----+
AID          | Type          | SN          | Password    | Status      | Image Active | Version     | Vendor/Model |
-----+-----+-----+-----+-----+-----+-----+-----+-----+
ont-3-1-1    | Config 5A5958454150002E | 1234567890 | 1234567890 | Active      | 1             | 100AAZC0b4 | ZYXE         |
              | Actual 5A5958454150002E | 1234567890 | 1234567890 | IS          | 2             | 100AAZC0C0 |              |
              | Details       |             |             |             |             |             |             |
              | Status       |             |             |             |             |             |             |
              | Estimated distance |             |             |             |             |             |             |
              | OMCI GEM port |             |             |             |             |             |             |
              | Model        |             |             |             |             |             |             |
              | Full bridge   |             |             |             |             |             |             |
              | Alarm profile |             |             |             |             |             |             |
              | Anti MAC Spoofing |             |             |             |             |             |             |
              | Planned Version |             |             |             |             |             |             |
              | Description   |             |             |             |             |             |             |
              | Management IP Address |             |             |             |             |             |             |
              | Wan 1        |             |             |             |             |             |             |
              | Type         |             |             |             |             |             |             |
              | Status      |             |             |             |             |             |             |
              | Nat         |             |             |             |             |             |             |
              | Service Type |             |             |             |             |             |             |
              | Vlan        |             |             |             |             |             |             |
              | Priority     |             |             |             |             |             |             |
              | Auto get IP  |             |             |             |             |             |             |
              | IP address   |             |             |             |             |             |             |
              | IP Mask     |             |             |             |             |             |             |
              | Gateway     |             |             |             |             |             |             |
              | Primary DNS  |             |             |             |             |             |             |
              | Second DNS  |             |             |             |             |             |             |
              | Wan 2       |             |             |             |             |             |             |
              | Wan 3       |             |             |             |             |             |             |
              | Wan 4       |             |             |             |             |             |             |
-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

From the information displayed we can verify several information such as the Serial Number, Password, Status (IS = In Service), Version (Firmware version, active version displays the letter “v”), Estimated distance in meter, and the model (5= PMG5318-B20B).

After we have verified the ONT status shows in Service, we may proceed to check the ONT card status

```
Show remote ontcard ontcard-<slot>-<port>-<ontID>-3
```

```

OLT2406# show remote ontcard ontcard-3-1-1-3
-----+-----+-----+-----+-----+-----+-----+-----+
AID          | Status AdminState | ExpType     | ActType ExpPort ActPort |
-----+-----+-----+-----+-----+-----+-----+
ontcard-3-1-1-3 | IS Unlocked      | VEIP        | VEIP 1 1             |
-----+-----+-----+-----+-----+-----+-----+-----+

```

At this point we may verify the status of the card to be In Service(IS), and that we have setup the correct type of card (VEIP).

After we have checked the status of the ONT card is in service and that we have selected the correct type of card, we may proceed to check the ontvenet status.

```
Show remote ontvenet
```



```

OLT2406# show remote ontvenet
AID | Config Status
-----|-----
ontvenet-3-1-1-3-1 | Active IS
ontvenet-3-1-10-2-1 | Active OOS-CO
ontvenet-3-1-125-4-1 | Active OOS-CO
ontvenet-3-1-127-2-1 | Active OOS-CO
ontvenet-3-1-128-2-1 | Active OOS-CO
    
```

The status should show IS (In Service) for the ONT being setup.

Finally, we can verify the UNI port queue setup, and VLAN status.

```

Show remote uniport uniport-<slot>-<port>-<ontID>-3-1 queue
Show remote uniport uniport-<slot>-<port>-<ontID>-3-1 vlan
    
```

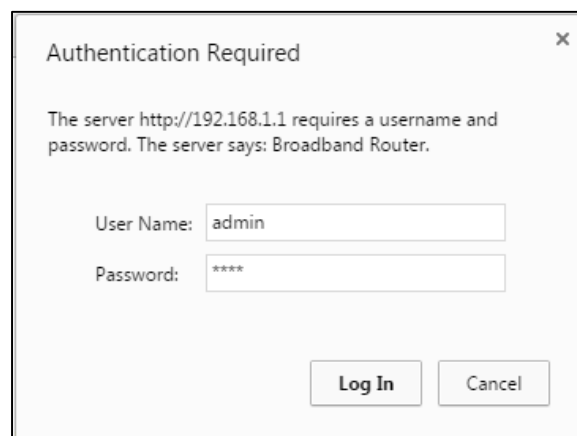
```

OLT2406# show remote uniport uniport-3-1-1-3-1 queue
Uniport TrafficClass Priority Weight UsBwProfileName DsBwProfileName DsOption BwShareGroupId
-----|-----|-----|-----|-----|-----|-----|-----
uniport-3-1-1-3-1 0 0 0 10M 10M olt 1
OLT2406# show remote uniport uniport-3-1-1-3-1 vlan
|AID | UNI-VID | Status | NNI-VID | Tag | PBit_Prof | DSCP_to_PBIT | Ing_Prof | TC | GemP | AES_Ept
-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----
v|uniport-3-1-1-3-1 | 100 | IS | 100 | tag | inactive | | alltc0 | 0 | 259 | disable
    
```

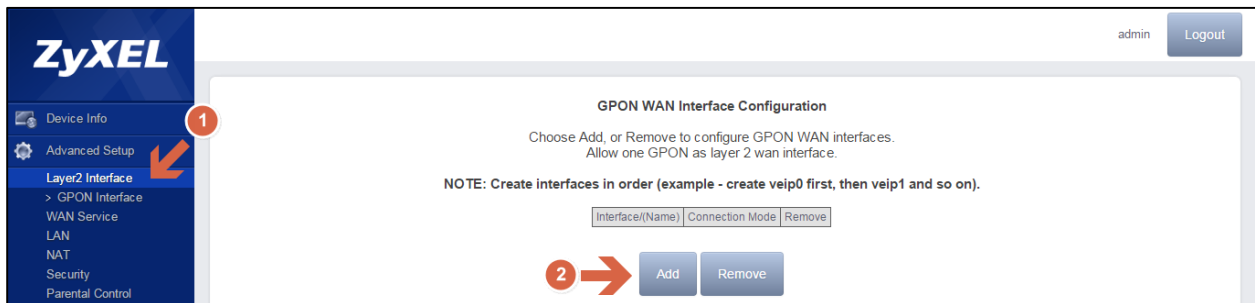
ONT Web GUI Setup

The ONT web GUI contains all the general setup required to establish communication services such as Internet, VoIP, video, and Wi-Fi. In this section we will explore the setup of Internet service.

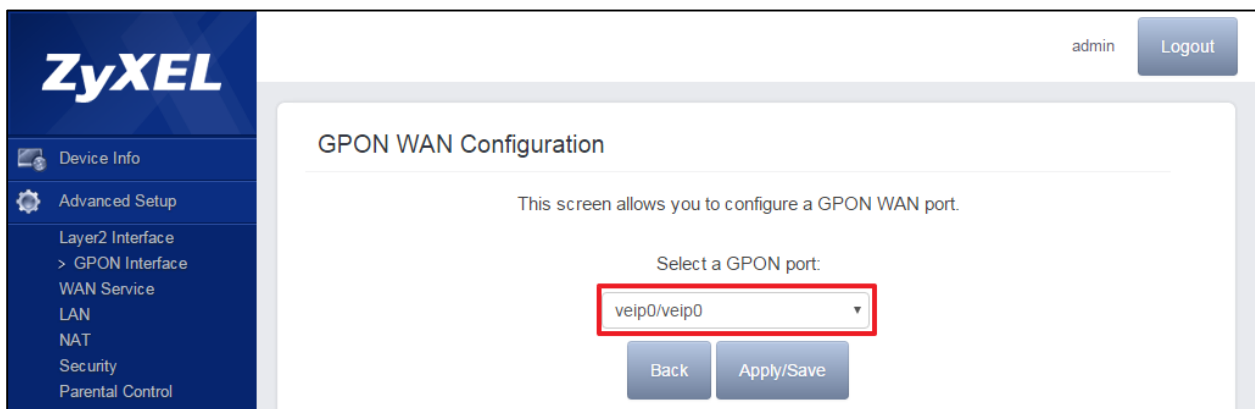
To access the web GUI, connect to any Lan Port of the ONT and after getting an IP for your PC navigate to <http://192.168.1.1>, access using the default username admin and password 1234.



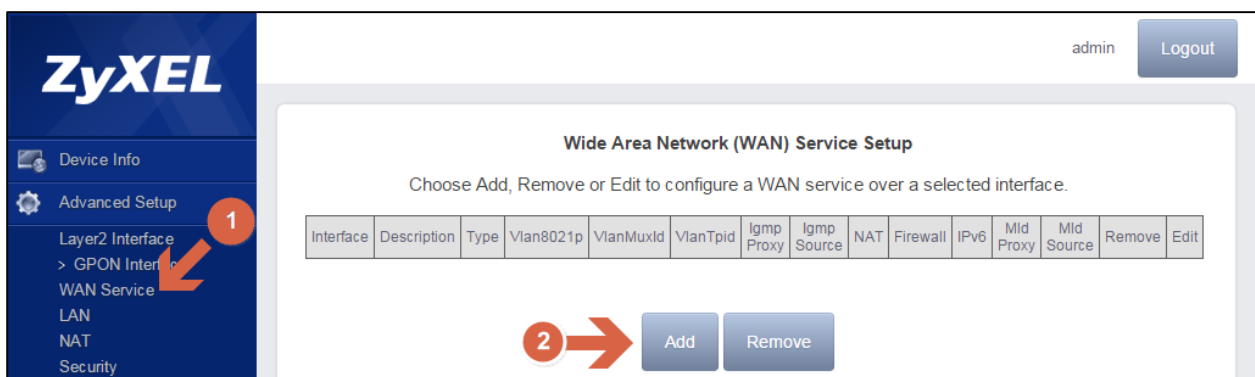
To configure GPON WAN interface go to **Advanced Setup > Layer 2 Interface**, click on the Add button.



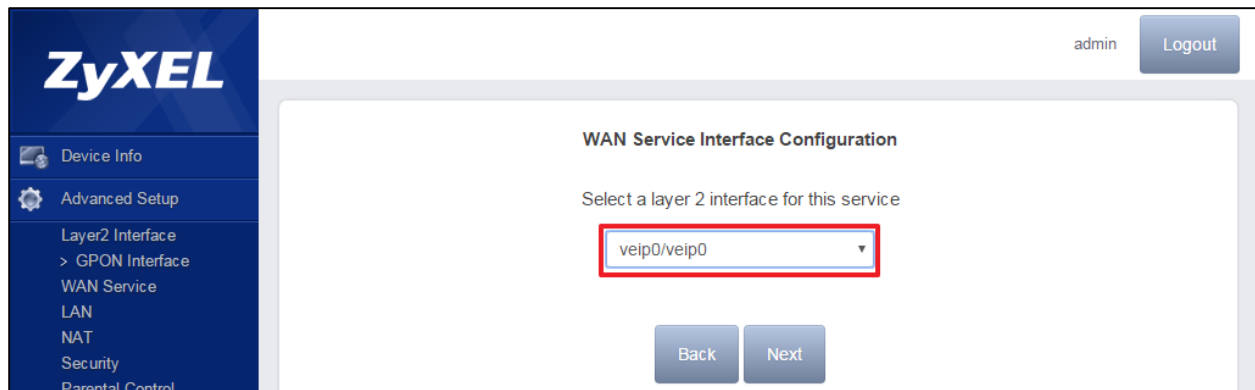
Select the GPON port as veip0/veip0 from the drop-down menu and click Apply/Save to create the new interface.



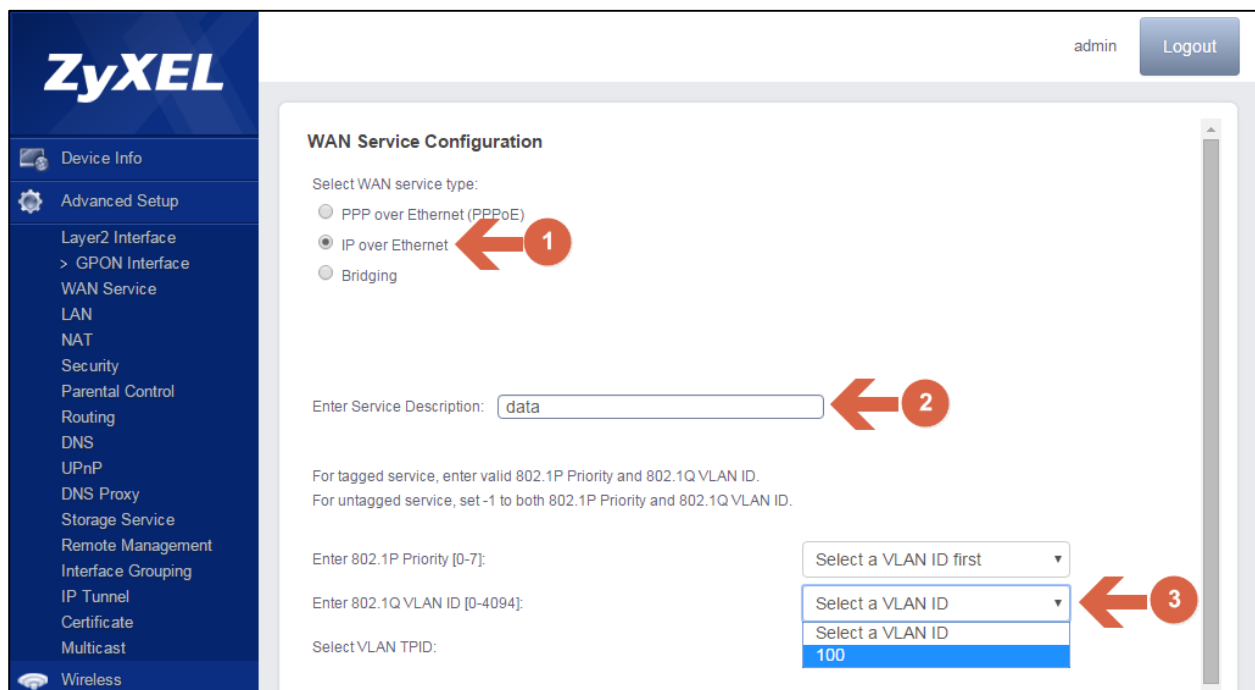
To configure the WAN service for the recently created interface go to **Advanced Setup > WAN Service**, click on the Add button.



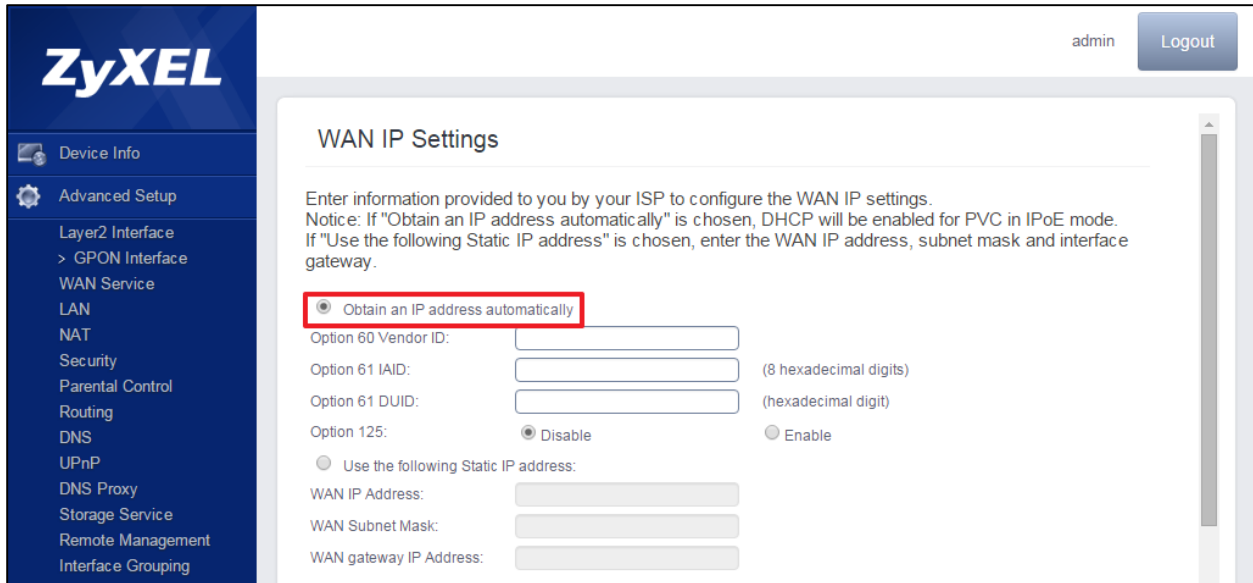
Select the interface recently created veip0/veip0:



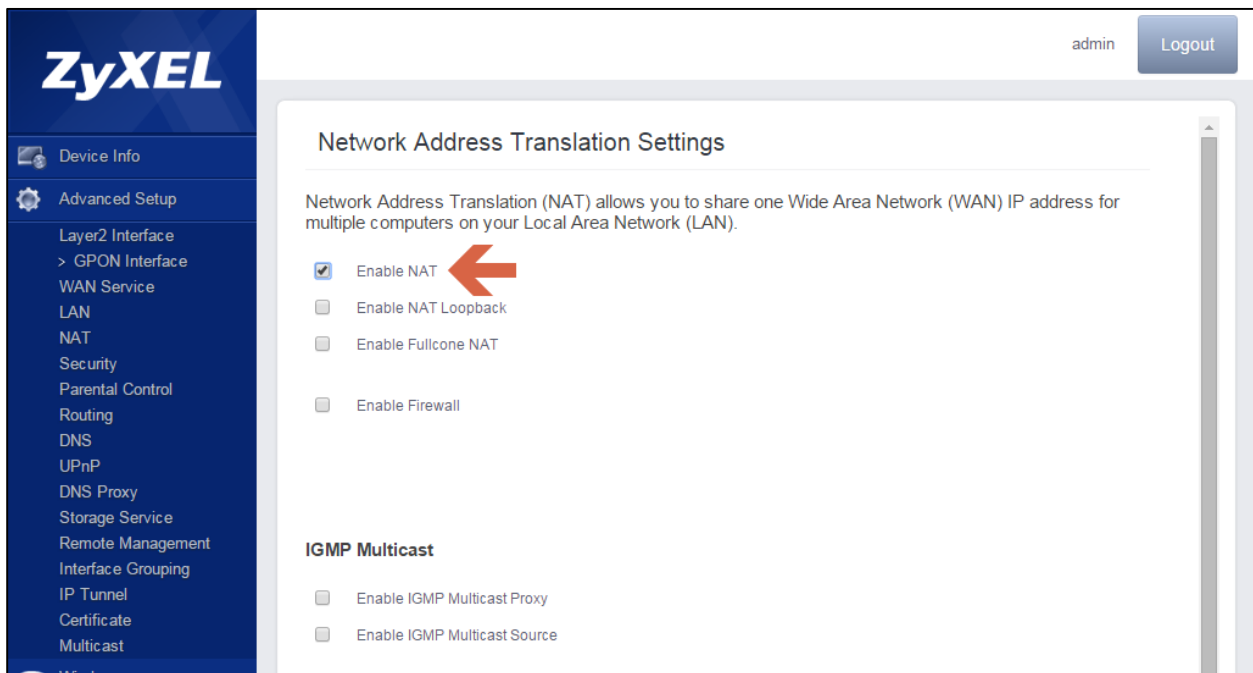
In this example we will create a service using IP over Ethernet (IPoE). First, proceed to select IP over Ethernet. Then, input the service description or leave the default value. Finally, select the VLAN ID and click next.



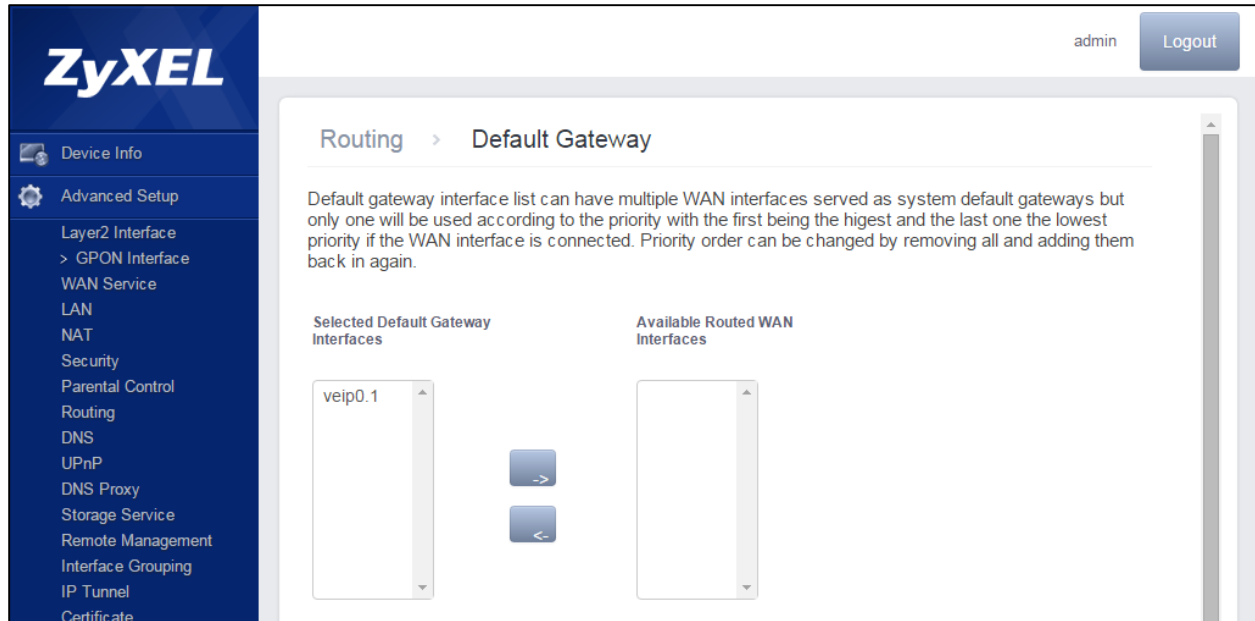
In the next screen you are prompted to choose between obtaining an IP address automatically or using a static IP. For our example, we will setup to obtain an IP address automatically, therefore we will only click next.



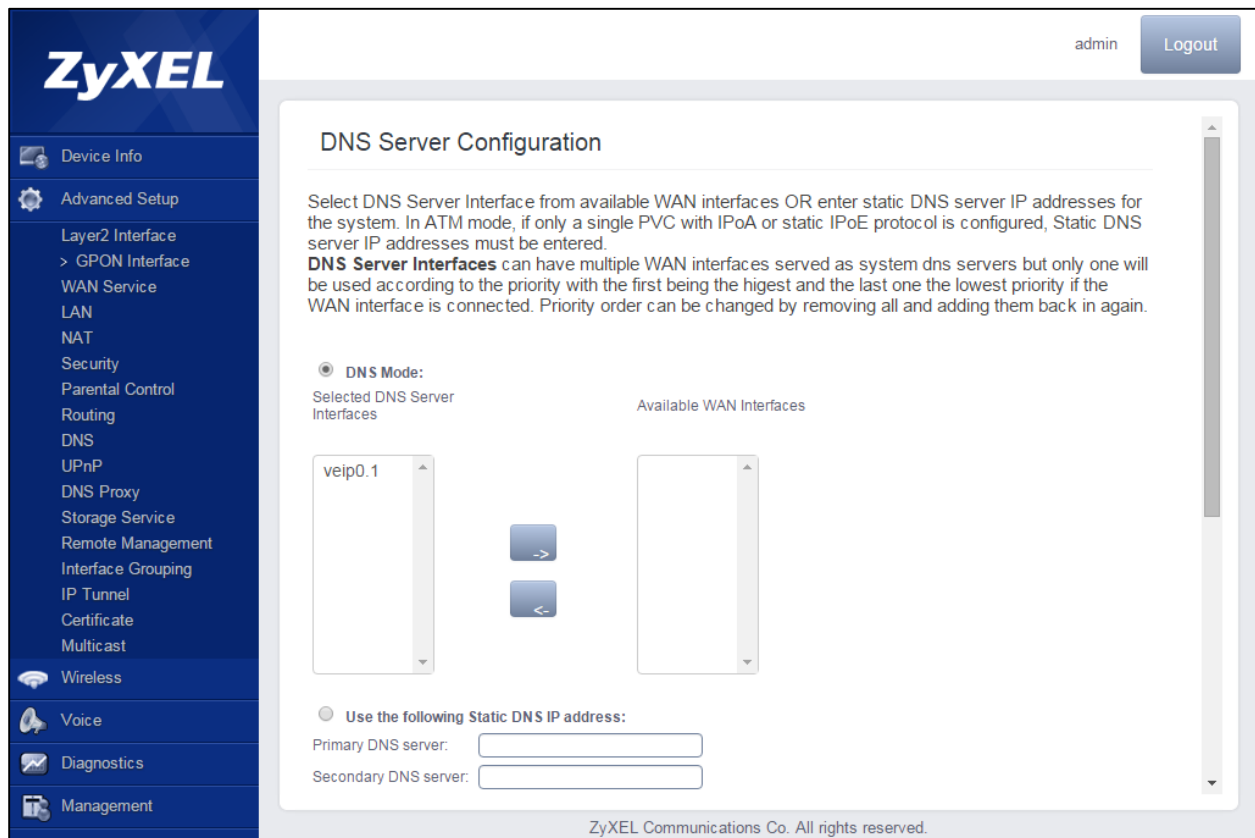
We will be prompted with the screen to setup the Network Address Translation Settings. In this example, we will share one WAN IP address for multiple computers on the LAN, therefore we will enable NAT and leave all other check boxes clear.



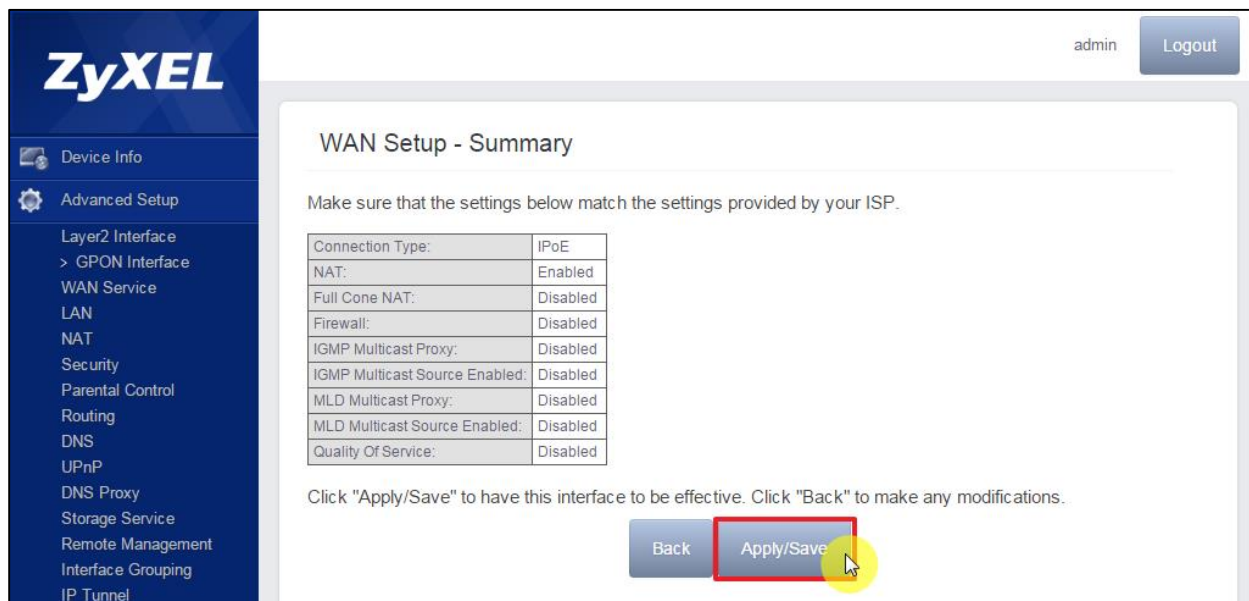
The Default Gateway screen will let you choose an interface as the default gateway. In this case we only have one interface, therefore we will only click next.



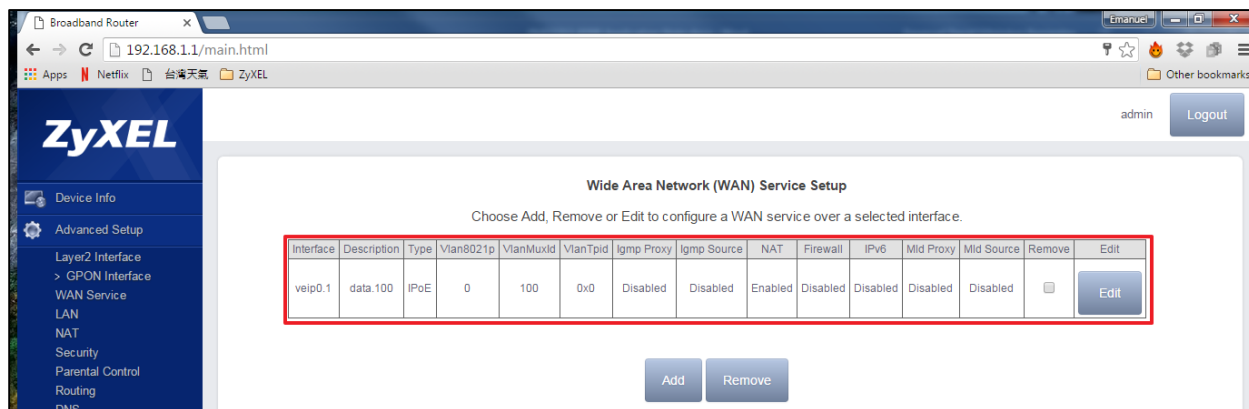
In the next screen we will be prompted to select the interface to automatically obtain the DNS Server configuration, or the option to set a static DNS IP address. In this example we will set the DNS mode and click next.



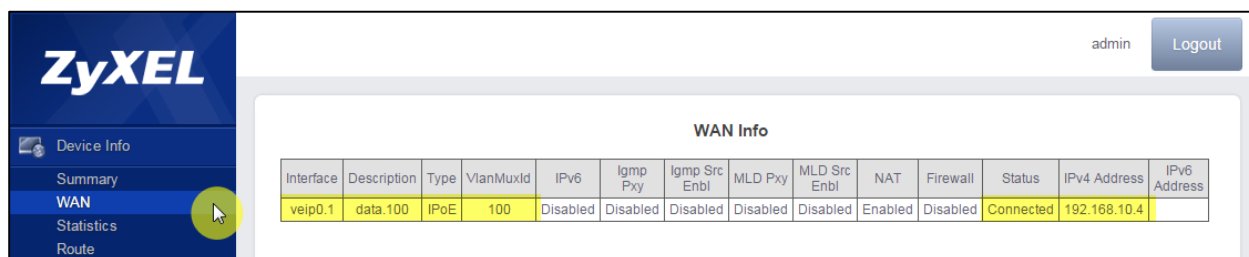
Finally, the WAN Setup summary screen will present to review the settings and apply/save the changes.



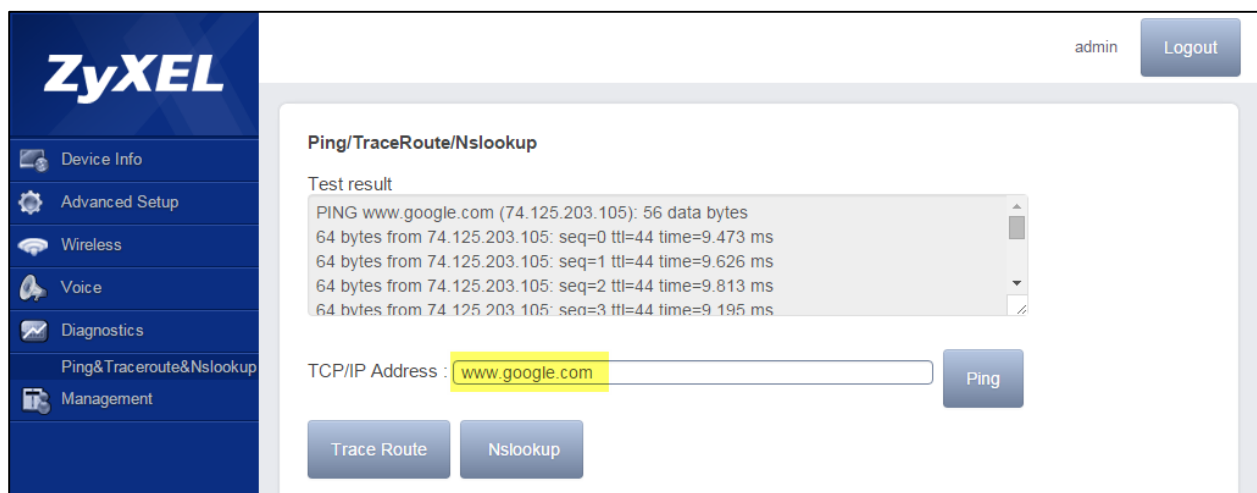
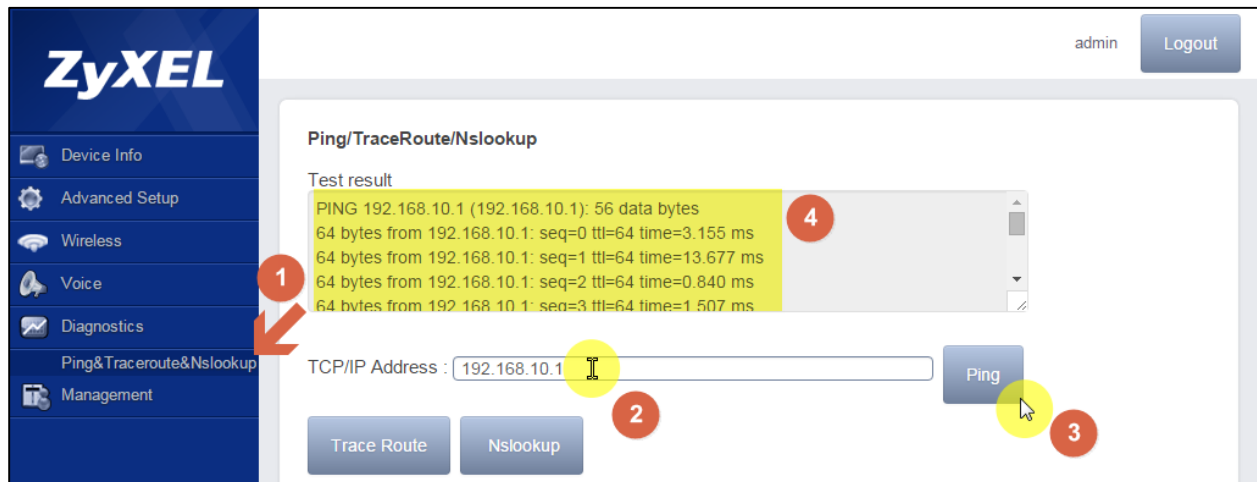
At this point we have successfully setup the Internet service.



It is possible to verify the WAN interface status, and IP address by going to **Device Info > WAN**.

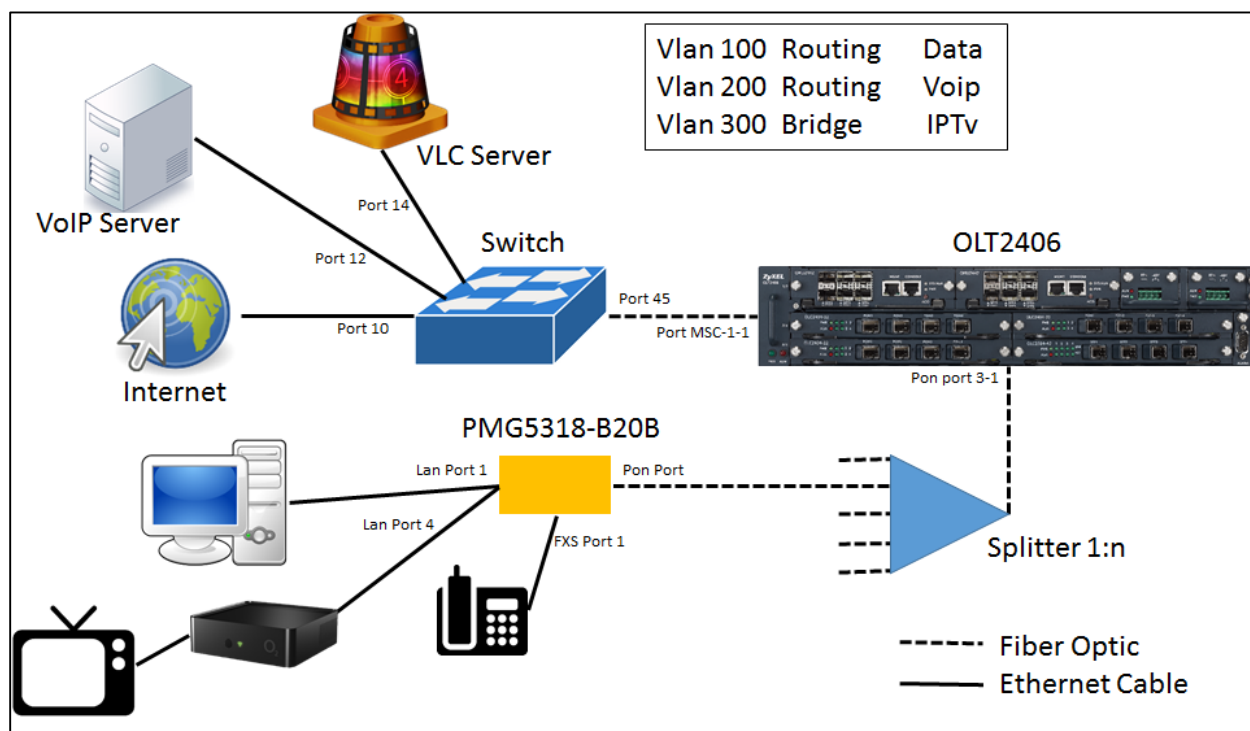


It is possible to verify the status by running a ping diagnostic by going to **Diagnostics > Ping & Traceroute & Nslookup**. Then input the IP address of your internet gateway or the URL of your preferred website.



General Scenario 2: Triple Play

In this scenario we will configure ZyXEL's Switch, OLT and ONT for Triple Play service. The ISP may provide "triple play" service to the GPON device. This allows you to take advantage of such features as broadband Internet access, voice over IP telephony and streaming video/audio media all at the same time with no noticeable loss in bandwidth.



Example Devices

- OLT: OLT2406, FW: 4.00(AAVA.4)C0
- ONT: PMG5318-B20B, FW: 100AAZC0C0
- Switch: GS2200-48

Switch Setup

Switch web GUI > Advanced Application > VLAN > Static VLAN

1. Check Active Box.
2. Set the name for the VLAN.
3. Set the VLAN Group ID. (VLAN ID).
4. Select the ports to be members of this VLAN as Fixed and select the port to be Tagged or Untagged.

5. Click the “Add” button at the end of the page to save your changes.

Static VLAN VLAN Status

1 ACTIVE

2 Name Data

3 VLAN Group ID 100

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
...		
44	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
45	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
46	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
47	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
48	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
49	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
50	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

5

In this example, switch port 9 and 10 will be used for access traffic (to internet) and port 45 will be used for the tagged traffic (to the OLT) using VLAN 100.

It is possible to check the current status of the VLAN by accessing:

Switch web GUI > Advanced Application > VLAN

Then proceed to click the index number for the VLAN ID you wish to verify.

VLAN Status		VLAN Port Setting		Static VLAN	
The Number of VLAN = 3					
Index	VID	Elapsed Time	Status		
1	1	94:43:49	Static		
2	100	94:38:49	Static		
3	2302	94:39:25	Static		

A new page will show containing the port diagram and the status of each port where “U” is Untagged and “T” is Tagged.

VLAN Detail		VLAN Status																									
VID	Port Number																				Elapsed Time	Status					
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40			42	44	46	48	50
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49			
100	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	94:42:33	Static
	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		

We will repeat the same procedure for VLANs 200 and 300 for their respective ports:

VLAN Detail		VLAN Status																									
VID	Port Number																				Elapsed Time	Status					
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40			42	44	46	48	50
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49			
200	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	124:37:24	Static
	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		

VLAN Detail		VLAN Status																									
VID	Port Number																				Elapsed Time	Status					
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40			42	44	46	48	50
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49			
300	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	124:38:15	Static
	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		

For the untagged ports, then proceed to add a PVID at the following location:

Switch web GUI > Advanced Application > VLAN > VLAN Port Settings

Set the PVID according to the VLAN membership:

VLAN Port Setting		Subnet Based Vlan	Protocol Based Vlan	VLAN Status	
GVRP <input type="checkbox"/>					
Port isolation <input type="checkbox"/>					
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All ▼	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
9	<input type="checkbox"/>	100	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
10	<input type="checkbox"/>	100	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
11	<input type="checkbox"/>	200	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
12	<input type="checkbox"/>	200	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
13	<input type="checkbox"/>	300	<input type="checkbox"/>	All ▼	<input type="checkbox"/>
14	<input type="checkbox"/>	300	<input type="checkbox"/>	All ▼	<input type="checkbox"/>

Ports 9, 10, 11, 12, 13, and 14 being untagged, proceed to setup their corresponding PVID. For port 45 no PVID is required, as it will be passing tagged traffic. Complete the setup by pressing “Apply” at the bottom of the page.

OLT2406 CLI Setup

How to read this section, in gray boxes you will find the executable CLI commands, meanwhile in yellow screenshots you’ll find the input of commands for example cases.

Setup Multicast VLAN Registration for IPTV service.

```

configure
mcast-channel 224.1.1.1 224.1.1.20 vlan 300 package-member 1 active on
exit
show mcast-channel
show mvr 300
    
```

```

OLT2406# configure
OLT2406(config)# mcast-channel 224.1.1.1 224.1.1.20 vlan 300 package-member 1 active on ←
OLT2406(config)# exit
OLT2406# show mcast-channel
multicast packages

  idx  vid  Start Address          active pkgMember preDur preCnt preBlackout pbit cacprof
  -----
  1    300  224.1.1.1              on 1          180   3     0           0
        224.1.1.20
        -
OLT2406# show mvr 300
MVLAN: 300   Active: Yes   Mode: Dynamic   802.1p Priority: 0
Name:
Source Port: msc-1-1, msc-1-2, msc-1-3, msc-1-4, msc-1-5, msc-1-6
Receiver Port:
Tagged Port: msc-1-1, msc-1-2, msc-1-3, msc-1-4, msc-1-5, msc-1-6
MVR Group Configuration:
Name          Start Address  End Address
-----
A0            224.1.1.1     224.1.1.20
OLT2406#

```

Adding a new PMG5318-B20B

To add a new ONT by CLI start by finding the Serial Number and Password after connecting the PON Port and turning on the device.

```
show remote ont unreg
```

```

OLT2406# show remote ont unreg
Pon_AID      | Type          SN              Password        Status
-----
pon-3-1      | UnReg 5A5958454150002E  1234567890     Active
OLT2406#

```

Now proceed to create a new ONT ID with the specification for the new ONT. For this example, a QoS Bandwidth profile named 10M with SIR 1024, AIR 5120, and PIR 10240 Kbps will be employed.

```

configure
remote ont ont-<slot>-<port>-<ontID>
sn xxxxxxxxxxxxxxxx
pa xxxxxxxxxxxx
model 5
bwgroup 1 ustype 5 usbwprofname 10M dsbwprofname 10M
no inactive
exit

```

```

OLT2406# configure
OLT2406(config)# remote ont ont-3-1-1
OLT2406(config-ont)# sn 5A5958454150002E
OLT2406(config-ont)# pa 1234567890
OLT2406(config-ont)# model 5
OLT2406(config-ont)# bwgroup 1 ustype 5 usbwprofname 10M dsbwprofname 10M
OLT2406(config-ont)# no inactive
OLT2406(config-ont)# exit

```

After creating the ONT-ID we will proceed to setup the ONT card, we will select card 3 which corresponds to the managed entity for router in the ONT, then we will define the type of card as VEIP (reference for router mode) and set the data ports as one.

```
remote ontcard ont-<slot>-<port>-<ontID>-3
cardtype VEIP data-port 1pa xxxxxxxxxx
no inactive
exit
```

```
OLT2406(config)# remote ontcard ontcard-3-1-1-3
OLT2406(config-ontcard)# cardtype VEIP data-port 1
OLT2406(config-ontcard)# no inactive
OLT2406(config-ontcard)# exit
```

After setting the router ONT card, we may activate the ontvenet as follow.

```
remote ontvenet ontvenet-<slot>-<port>-<ontID>-3-1
no inactive
exit
```

```
OLT2406(config)# remote ontvenet ontvenet-3-1-1-3-1
OLT2406(config-ontvenet)# no inactive
OLT2406(config-ontvenet)# exit
```

Finally, we will setup the UNI port queue and VLAN. For this example, a QoS ingress profile was defined with the name “alltc0” setting all priorities to traffic class 0.

```
remote uniport uniport-<slot>-<port>-<ontID>-3-1
queue tc 0 priority 0 weight 0 usbwprofname 10M dsbwprofname 10M dsoption olt bwsharegroupid 1
vlan 100 ing alltc0
vlan 200 ing alltc0
vlan 300 ing alltc0
igmpchannel 300 fullviewpkg 1
```

```
OLT2406# configure
OLT2406(config)# remote uniport uniport-3-1-1-3-1
OLT2406(config-remote-uniport)# queue tc 0 priority 0 weight 0 usbwprofname 10M dsbwprofname 10M dsoption olt bwsharegroupid 1
OLT2406(config-remote-uniport)# vlan 100 ing alltc0
OLT2406(config-remote-uniport)# vlan 200 ing alltc0
OLT2406(config-remote-uniport)# vlan 300 ing alltc0
OLT2406(config-remote-uniport)# igmpchannel 300 fullviewpkg 1
OLT2406(config-remote-uniport)# exit
OLT2406(config)# exit
```

Checking the ONT status

After completing the ONT setup, we can verify the status of its different elements.

```
Show remote ont ont-<slot>-<port>-<ontID>
```

```

OLT2406# sh remote ont ont-3-1-1
-----+-----+-----+-----+-----+-----+-----+-----+-----+
AID      | Type      SN          Password  Status  Image Active  Version  Vendor/Model
-----+-----+-----+-----+-----+-----+-----+-----+-----+
ont-3-1-1 | Config 5A5958454150002E 1234567890 Active | 1      100AAZC0b4 | ZYXE
          | Actual 5A5958454150002E 1234567890 IS    | 2      V      100AAZC0C0 |
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Details
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Status                : IS
          | Estimated distance    : 0 m
          | OMCI GEM port        : 128
          | Model                 : 5
          | Full bridge          : disable
          | Alarm profile         : DEFVAL
          | Anti MAC Spoofing    : disable
          | Planned Version      :
          | Description           :
          | Management IP Address : N/A
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Wan 1                 : Enable
          | Type                  : IPoE
          | Status                : Up
          | Nat                   : Enable
          | Service Type          : IPTV
          | Vlan                  : 100
          | Priority               : 0
          | Auto get IP           : Enable
          | IP address            : 192.168.10.4
          | IP Mask               : 255.255.255.0
          | Gateway               : 192.168.10.1
          | Primary DNS           : 192.168.10.1
          | Second DNS            : 0.0.0.0
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Wan 2                 : Disable
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Wan 3                 : Disable
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
          | Wan 4                 : Disable
          +-----+-----+-----+-----+-----+-----+-----+-----+-----+
    
```

From the information displayed, we can verify several information such as the Serial Number, Password, Status (IS = In Service), Version (Firmware version, active version displays the letter “v”), Estimated distance in meter, and the model (5= PMG5318-B20B).

After we have verified the ONT status shows in service, we may proceed to check the ONT card status

```
Show remote ontcard ontcard-<slot>-<port>-<ontID>-3
```

```

OLT2406# show remote ontcard ontcard-3-1-1-3
-----+-----+-----+-----+-----+-----+-----+-----+
AID      | Status AdminState  ExpType  ActType ExpPort ActPort
-----+-----+-----+-----+-----+-----+-----+-----+
ontcard-3-1-1-3 | IS Unlocked      VEIP     VEIP     1      1
-----+-----+-----+-----+-----+-----+-----+-----+
    
```

At this point we may verify the status of the card to be In Service(IS), and that we have setup the correct type of card (VEIP).

After we have checked the status of the ONT card is in service and that we have selected the correct type of card, we may proceed to check the ontvenet status.

```
Show remote ontvenet
```

```
OLT2406# show remote ontvenet
AID | Config Status
-----|-----
ontvenet-3-1-1-3-1 | Active IS
ontvenet-3-1-10-2-1 | Active OOS-CO
ontvenet-3-1-125-4-1 | Active OOS-CO
ontvenet-3-1-127-2-1 | Active OOS-CO
ontvenet-3-1-128-2-1 | Active OOS-CO
```

The status should show IS (in service) for the ONT being setup.

Finally, we can verify the UNI port queue setup, and VLAN status.

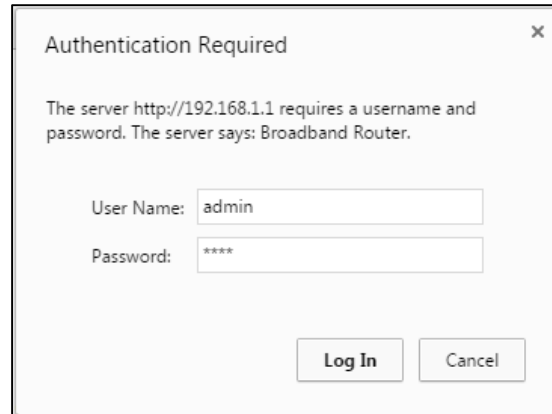
```
Show remote uniport uniport-<slot>-<port>-<ontID>-3-1 queue
Show remote uniport uniport-<slot>-<port>-<ontID>-3-1 vlan
Show remote uniport uniport-<slot>-<port>-<ontID>-3-1 igmpchannel
```

```
OLT2406# show remote uniport uniport-3-1-1-3-1 queue
Uniport TrafficClass Priority Weight UsBwProfileName DsBwProfileName DsOption BwS
-----|-----|-----|-----|-----|-----|-----|-----
uniport-3-1-1-3-1 0 0 0 10M 10M olt
OLT2406# show remote uniport uniport-3-1-1-3-1 vlan
|AID | UNI-VID | Status | NNI-VID | Tag | PBit_Prof | DSCP_to_PBIT | Ing_Prof | TC | GemP | AES_Ept
-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----
v|uniport-3-1-1-3-1 | 100 | IS | 100 | tag | inactive | | alltc0 | 0 | 256 | disable
v|uniport-3-1-1-3-1 | 200 | IS | 200 | tag | inactive | | alltc0 | 0 | 260 | disable
v|uniport-3-1-1-3-1 | 300 | IS | 300 | tag | inactive | | alltc0 | 0 | 261 | disable
OLT2406# show remote uniport uniport-3-1-1-3-1 igmpchannel
AID | Channel | Version | Maxgroup | Snooping | Cacprof | Maxmsg | Fullview_pkgs | Preview_pkgs
-----|-----|-----|-----|-----|-----|-----|-----|-----
uniport-3-1-1-3-1 | 300 | IGMPv2 | 64 | off | | 0 | 1 | -
OLT2406#
```

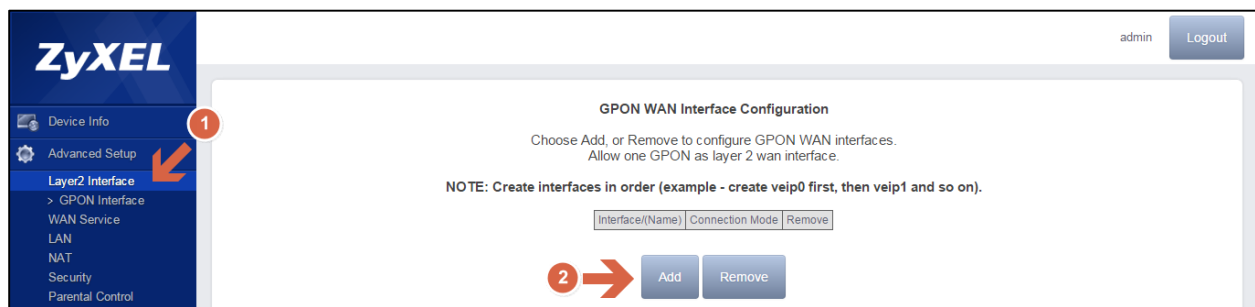
ONT Web GUI Setup

The ONT web GUI contains all the general setup required to establish communication services such as Internet, VoIP, video, and Wi-Fi. In this section we will explore the setup of Internet service.

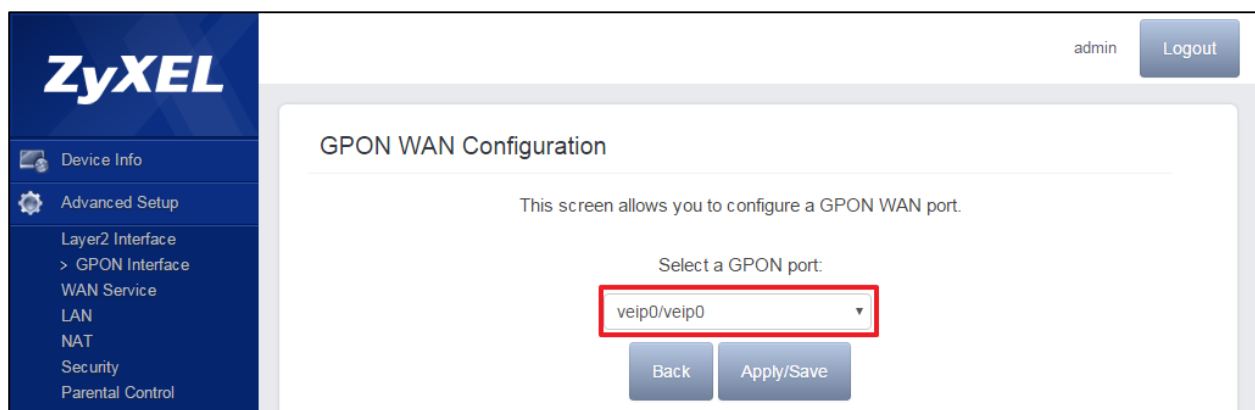
To access the web GUI, connect to any LAN port of the ONT and after getting an IP for your PC, open a browser to navigate to <http://192.168.1.1>, access using the default username “admin” and password “1234”.



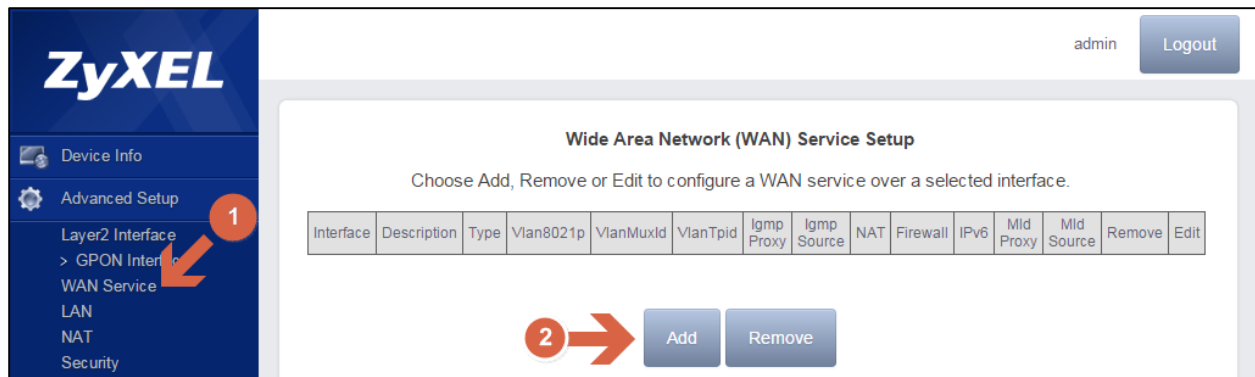
To configure GPON WAN interface go to **Advanced Setup > Layer 2 Interface**, click on the Add button.



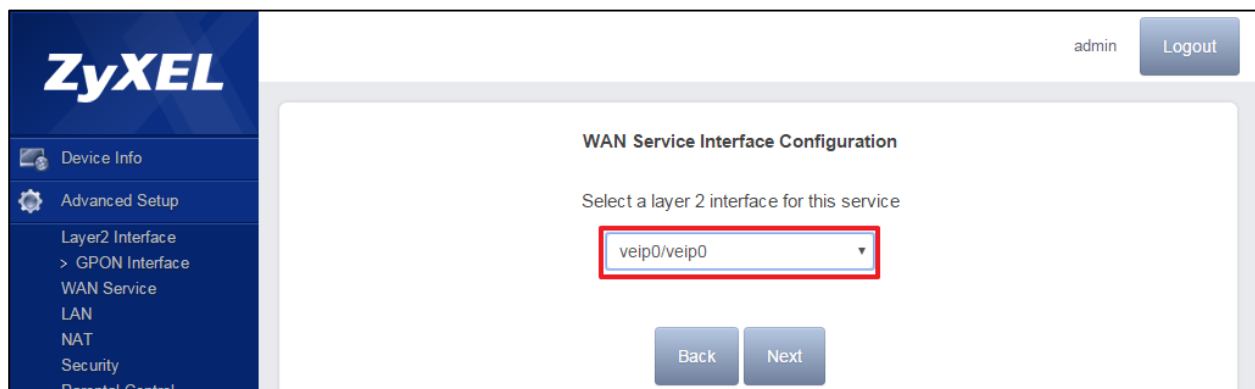
Select the GPON port as veip0/veip0 from the drop down menu and click Apply/Save to create the new interface.



To configure the WAN service for the Data service, go to **Advanced Setup > WAN Service**, click on the Add button.

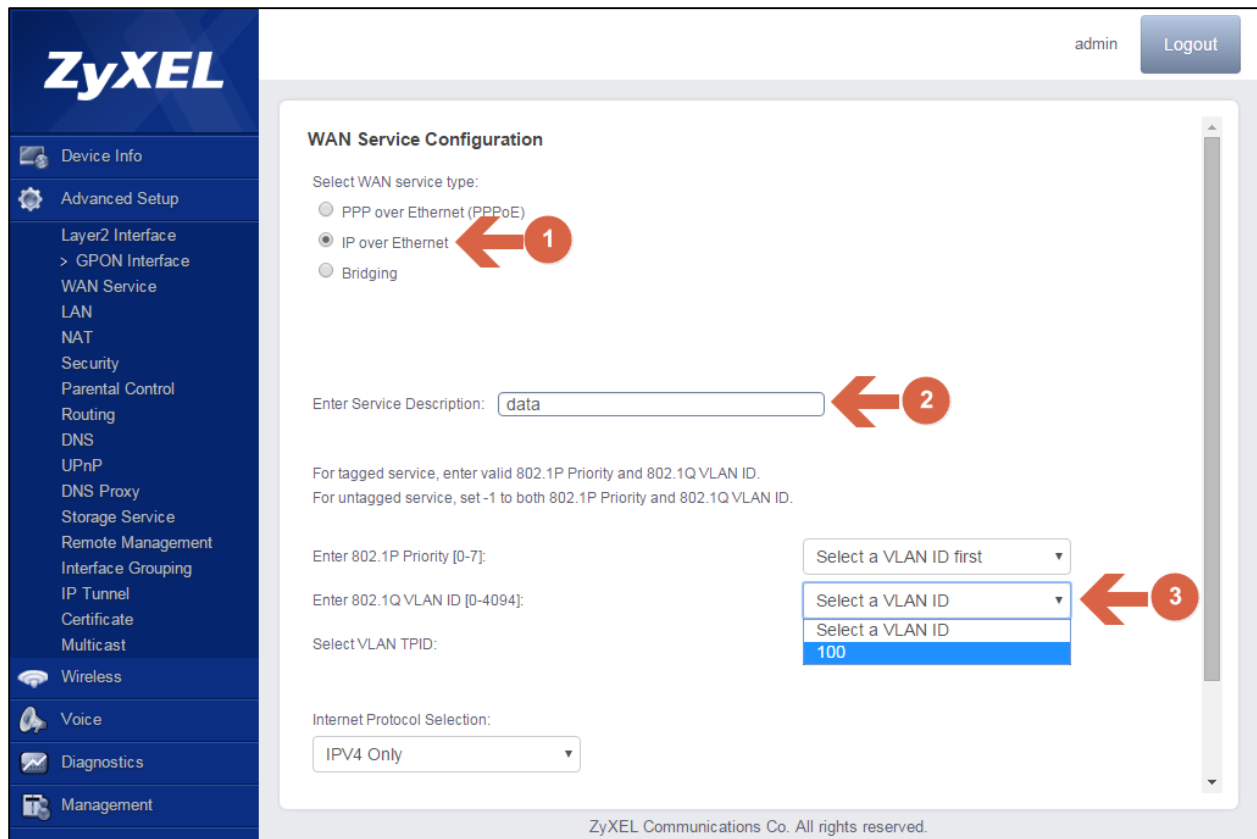


Select the interface recently created veip0/veip0:

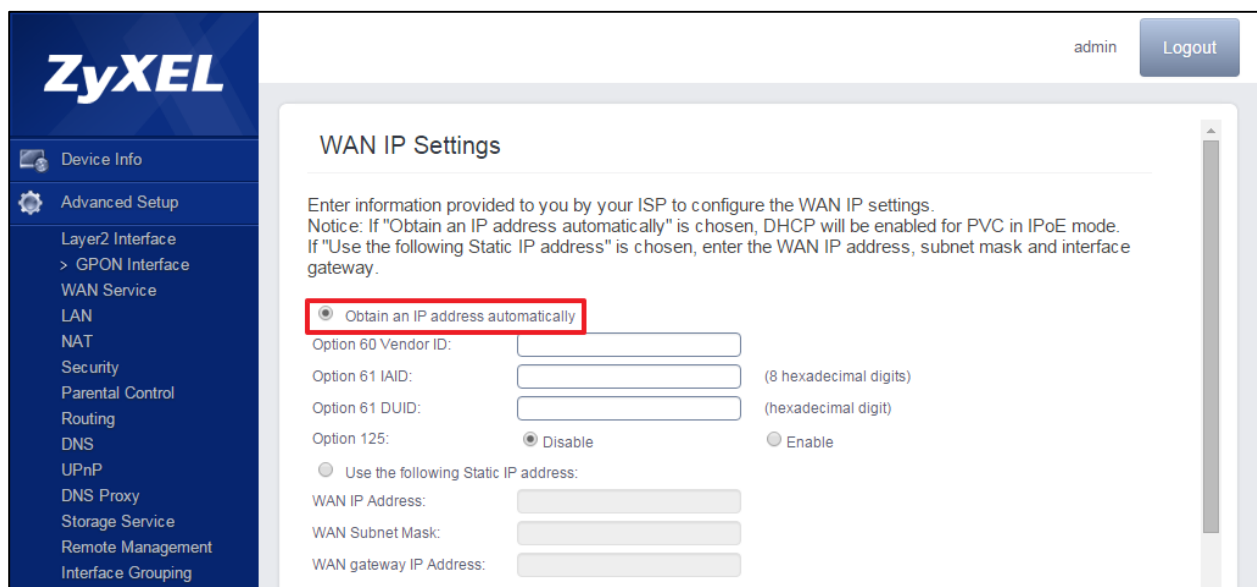


Data Service Setup

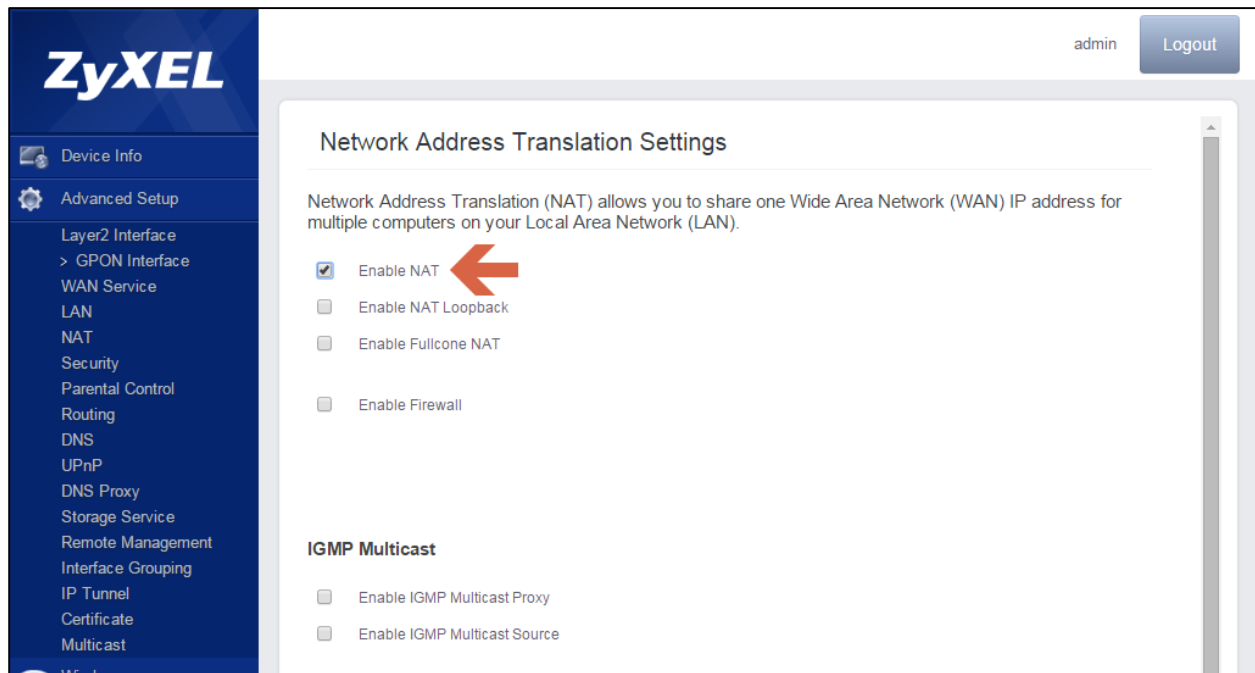
In this example we will create a service using IP over Ethernet (IPoE). First, proceed to select IP over Ethernet. Then, optionally input the service description. Finally, select the VLAN ID and click next.



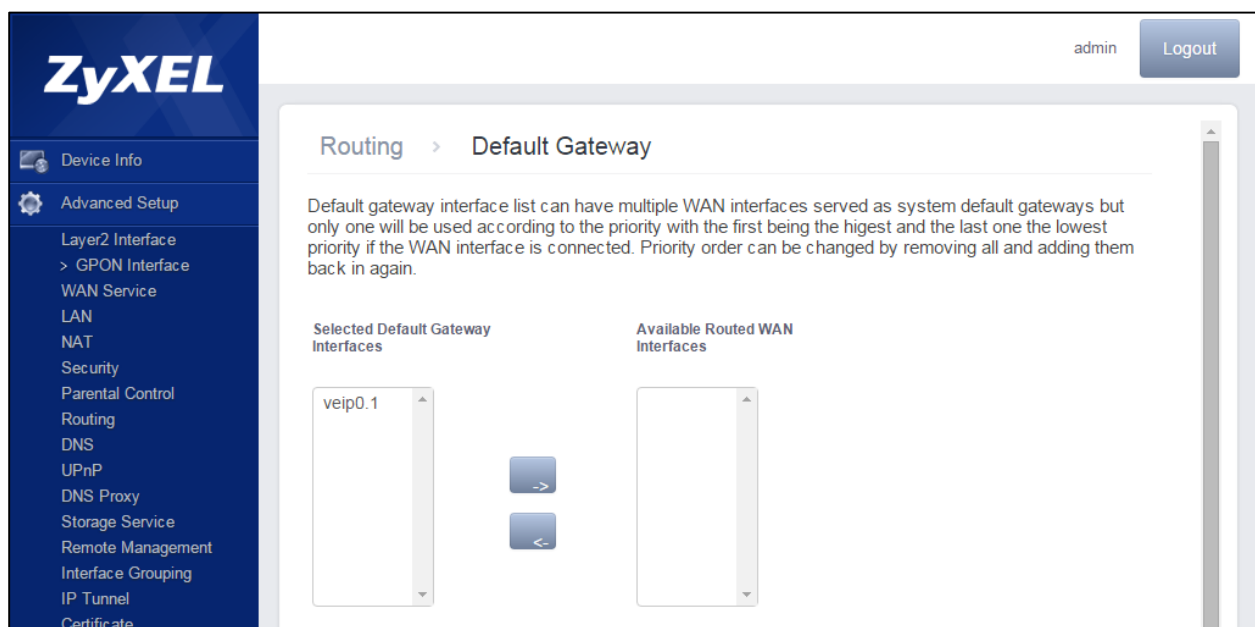
In the next screen you are prompted to choose between obtaining an IP address automatically or using a static IP. For our example, we will setup to obtain an IP address automatically. Therefore, we will only click next.



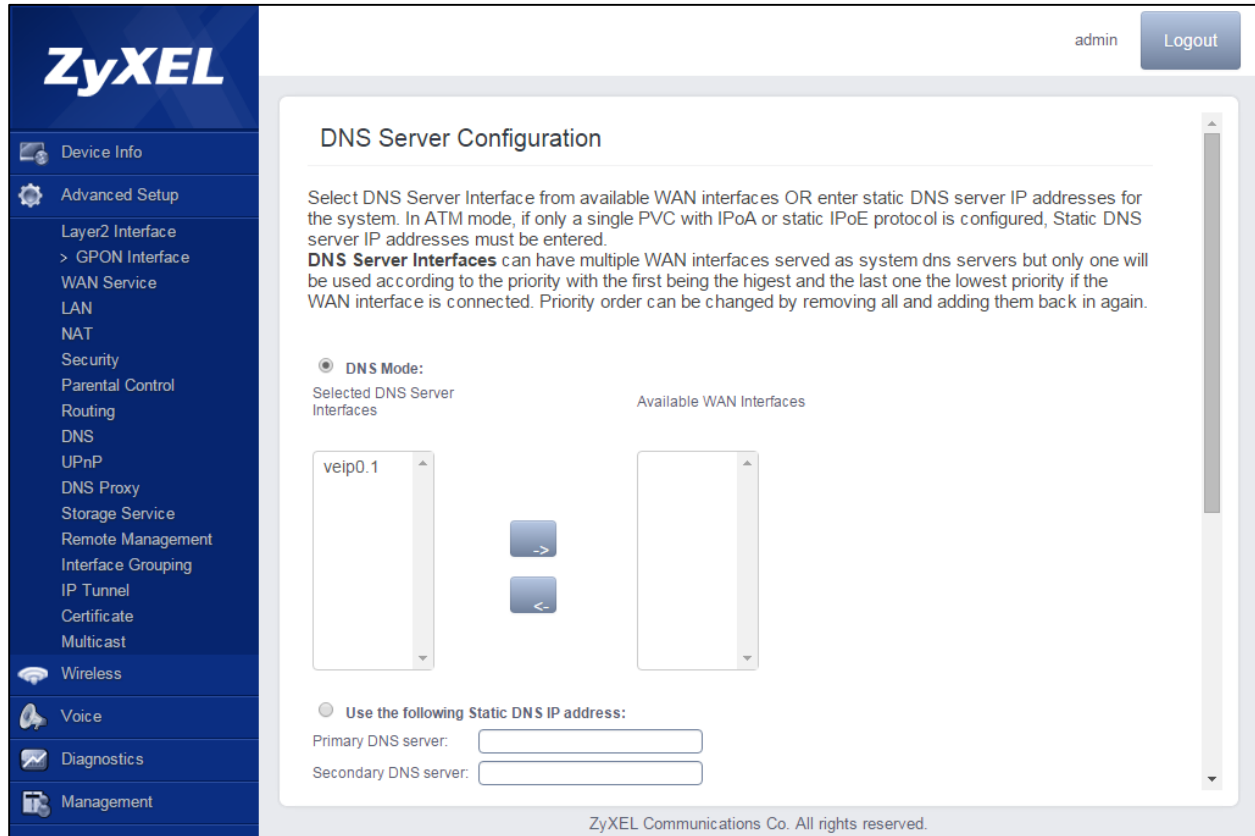
We will be prompted with the screen to setup the Network Address Translation Settings. In this example, we will share one WAN IP address for multiple computers on the LAN, therefore we will enable NAT and leave all other check boxes clear.



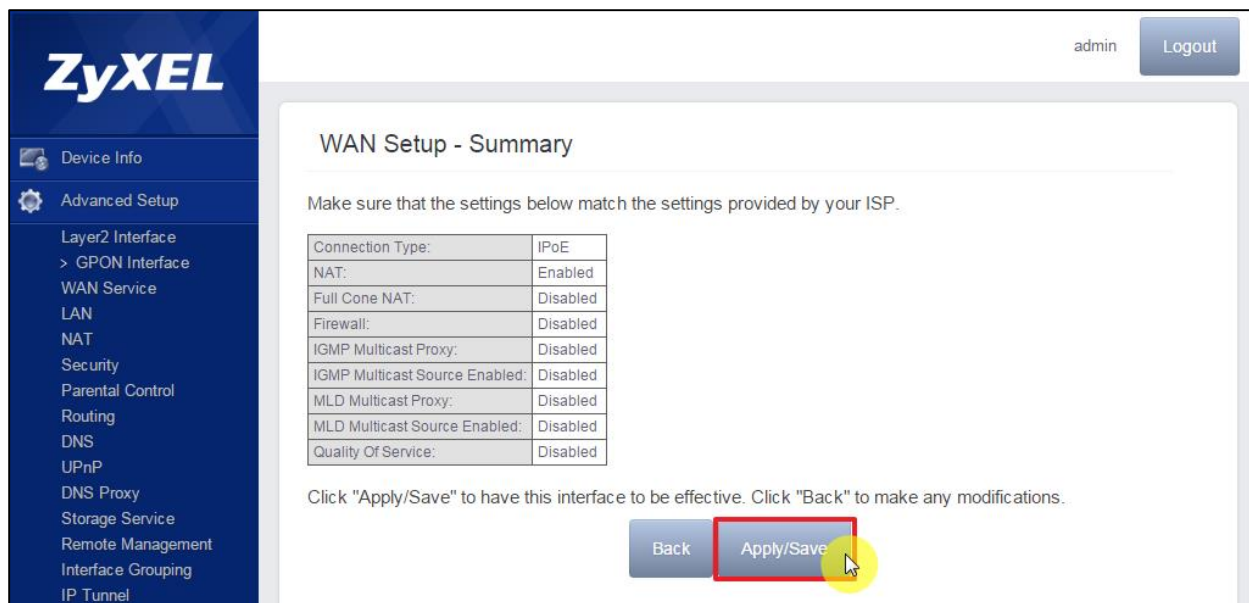
The Default Gateway screen will let you choose an interface as the default gateway. In this case we only have one interface, therefore we will only click next.



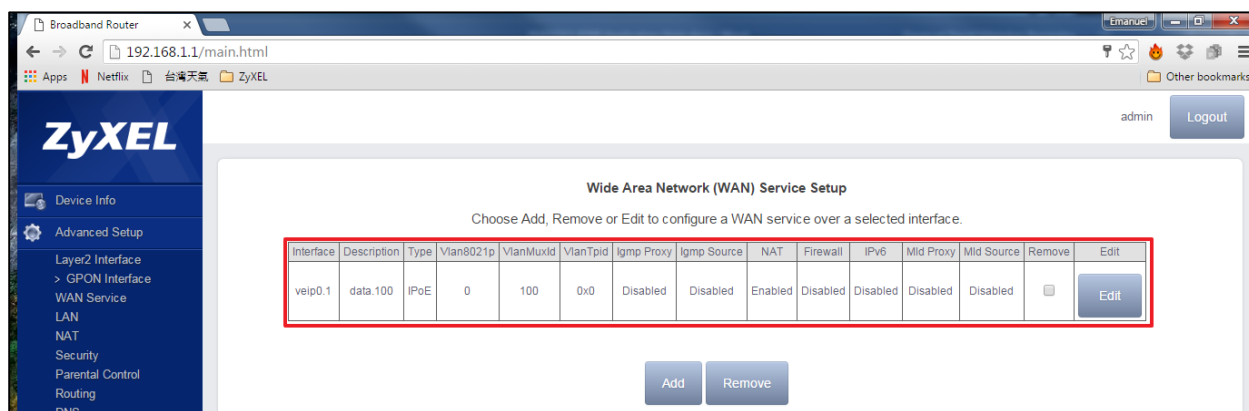
In the next screen we will be prompted to select the interface to automatically obtain the DNS Server configuration or the option to set a static DNS IP address. In this example we will set the DNS mode and click next.



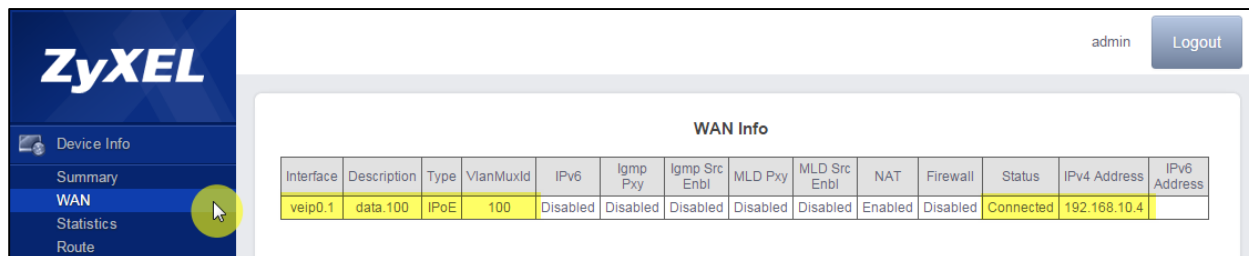
Finally, the WAN Setup summary screen will present to review the settings and apply/save the changes.



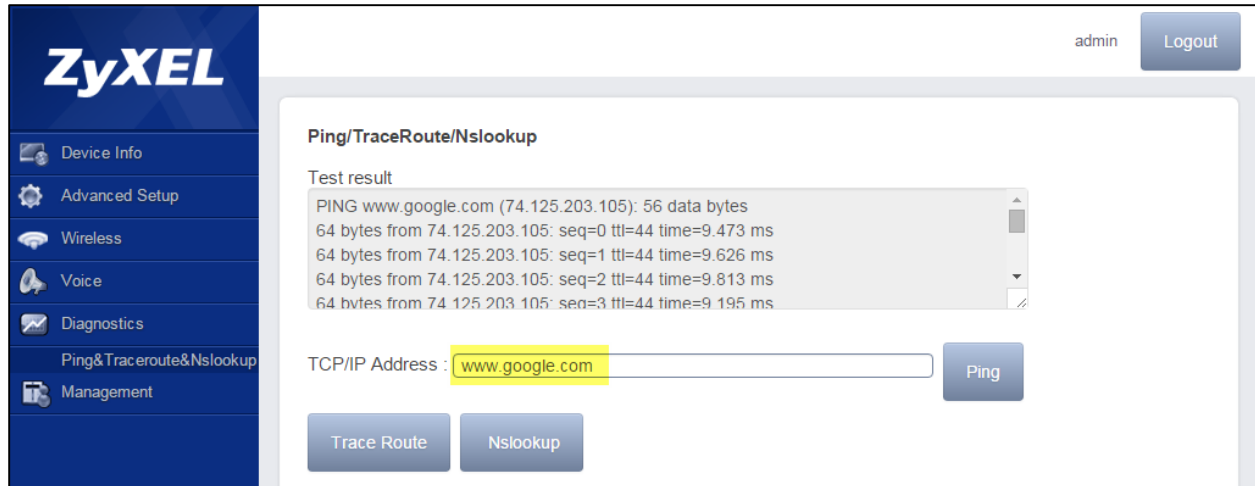
At this point we have successfully setup the Internet service.



It is possible to verify the WAN interface status and IP address by going to **Device Info > WAN**.

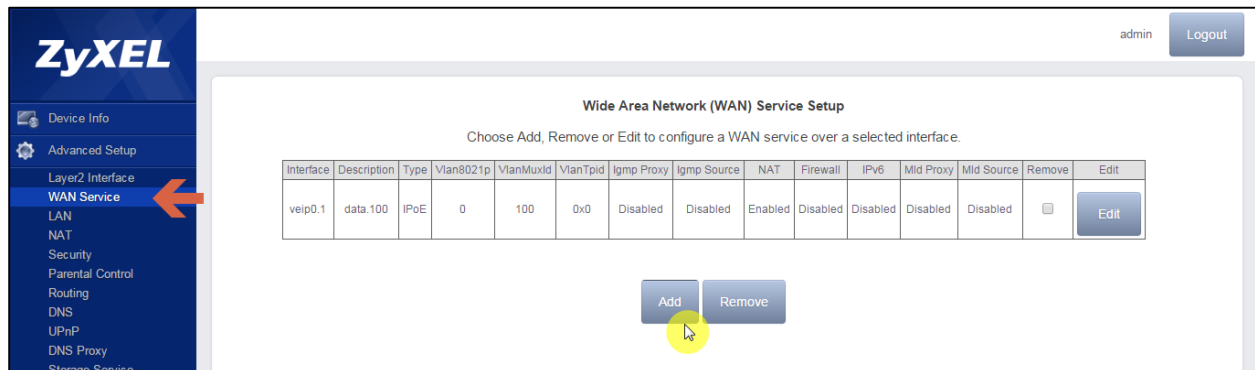


It is possible to verify the status by running a ping diagnostic by going to **Diagnostics > Ping & Traceroute & Nslookup**. Then input the IP address of your internet gateway or the URL of your preferred website.

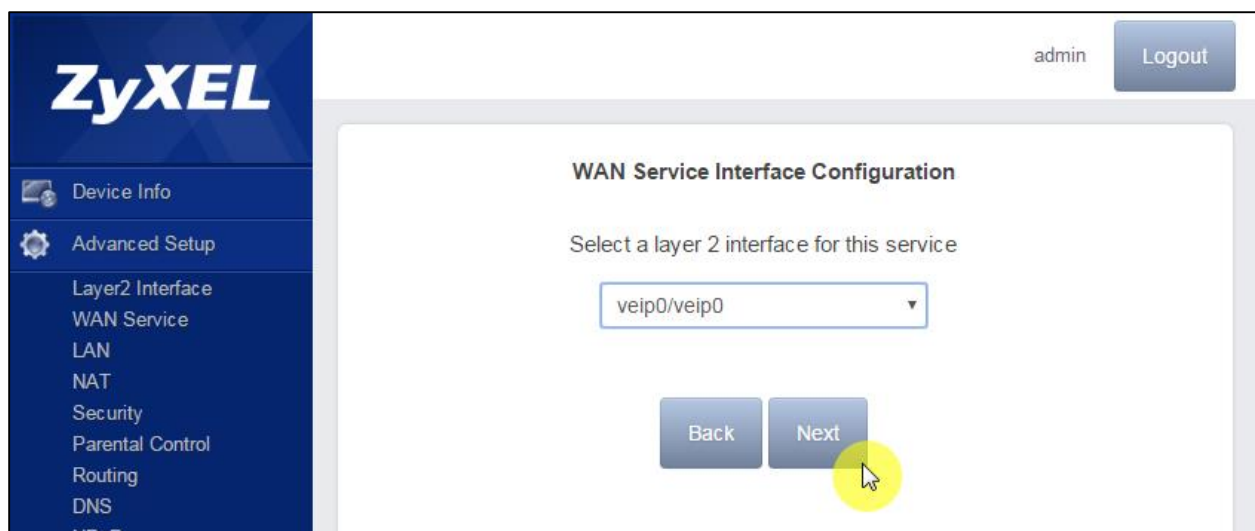


VoIP Service Setup

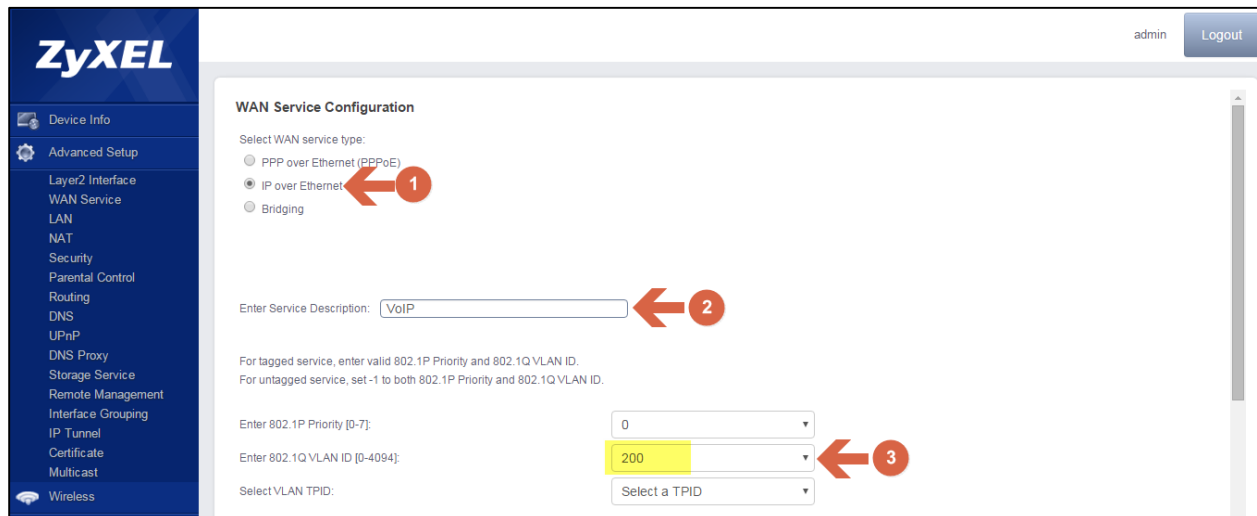
To configure the Voice service, we will proceed to add a new WAN service:



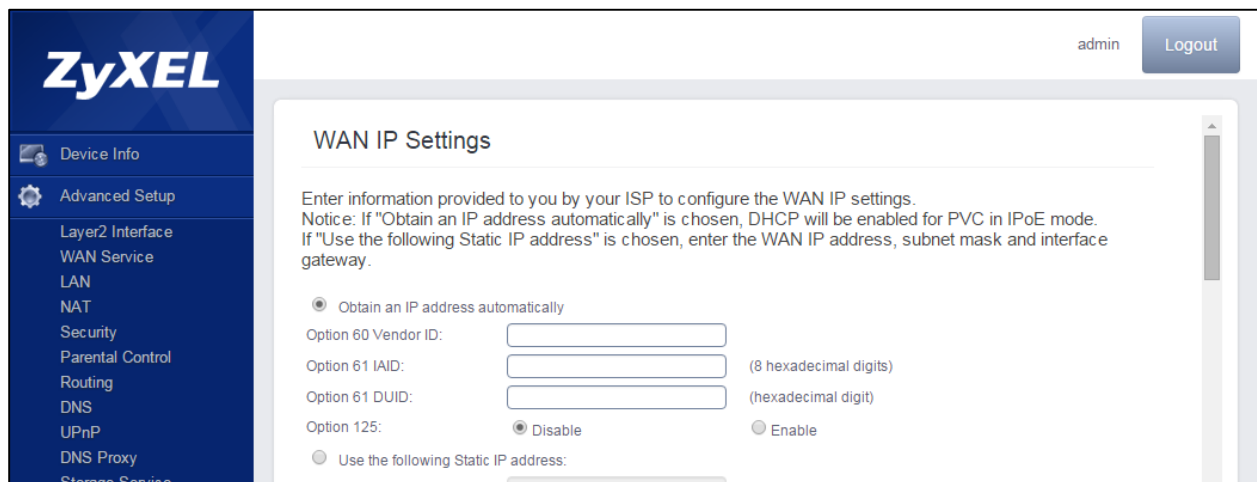
In the next screen click next:



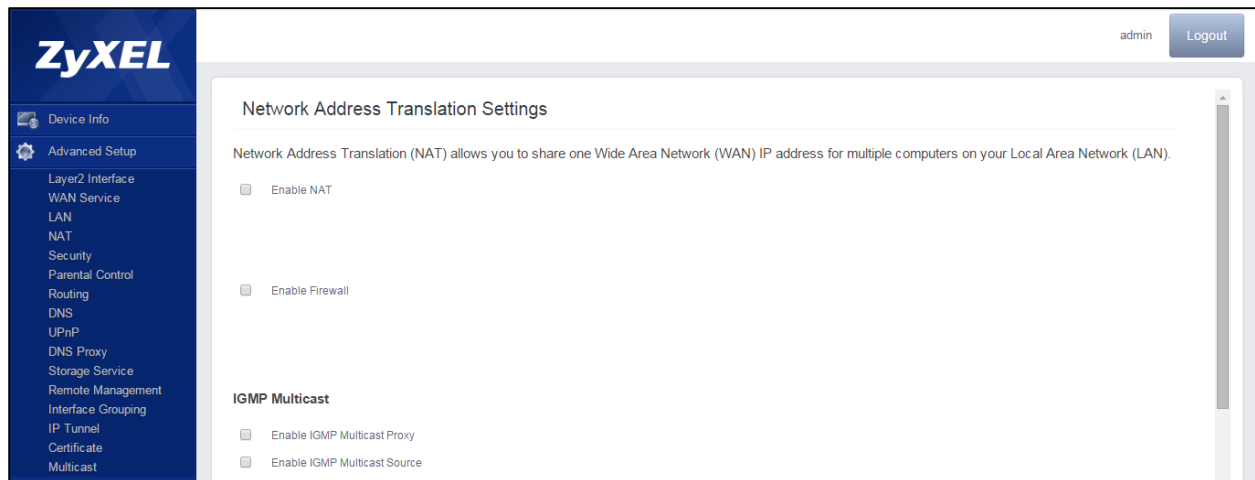
In the next screen we will setup the IP service type by selecting IP over Ethernet. Then, set the service name. Finally, select the VLAN ID corresponding to the VoIP service, in this case VID 200.



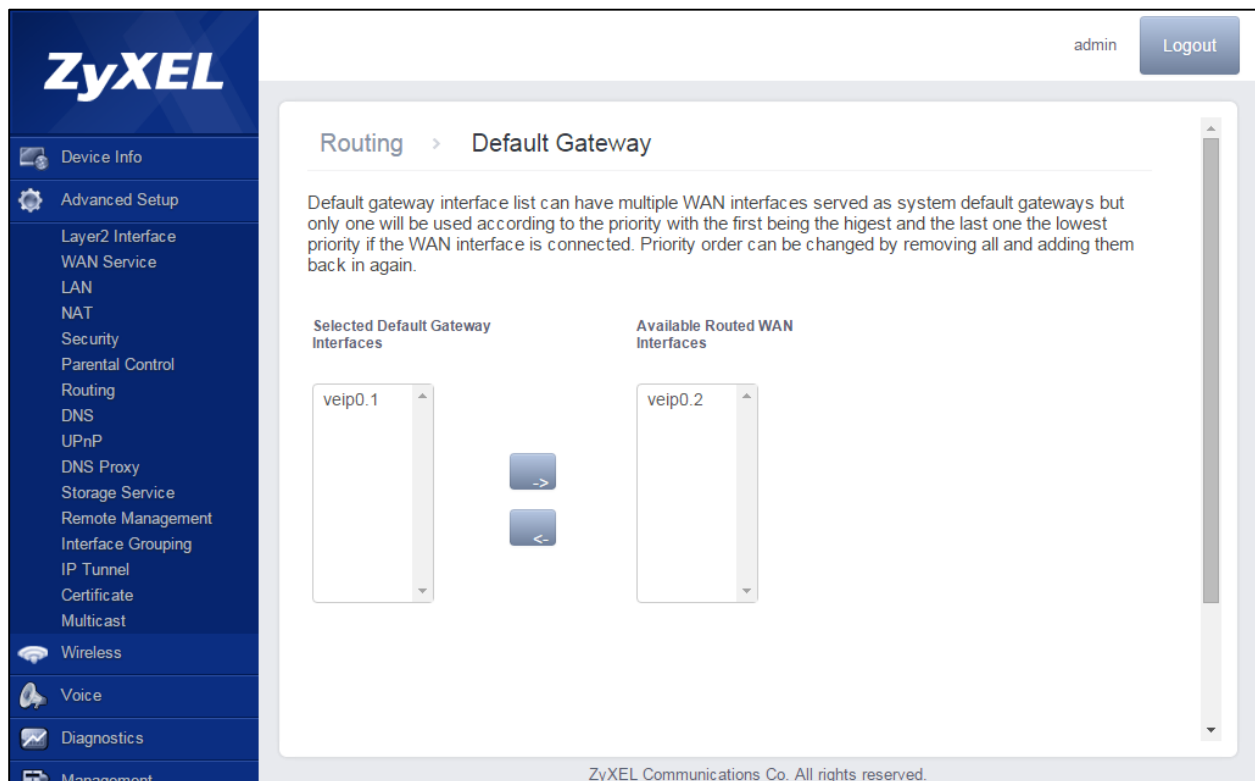
In the next screen, we will be requested to define to setup the IP configuration to be dynamic or static. For the purpose of this example it will be defined as automatic. Proceed to click on Next.

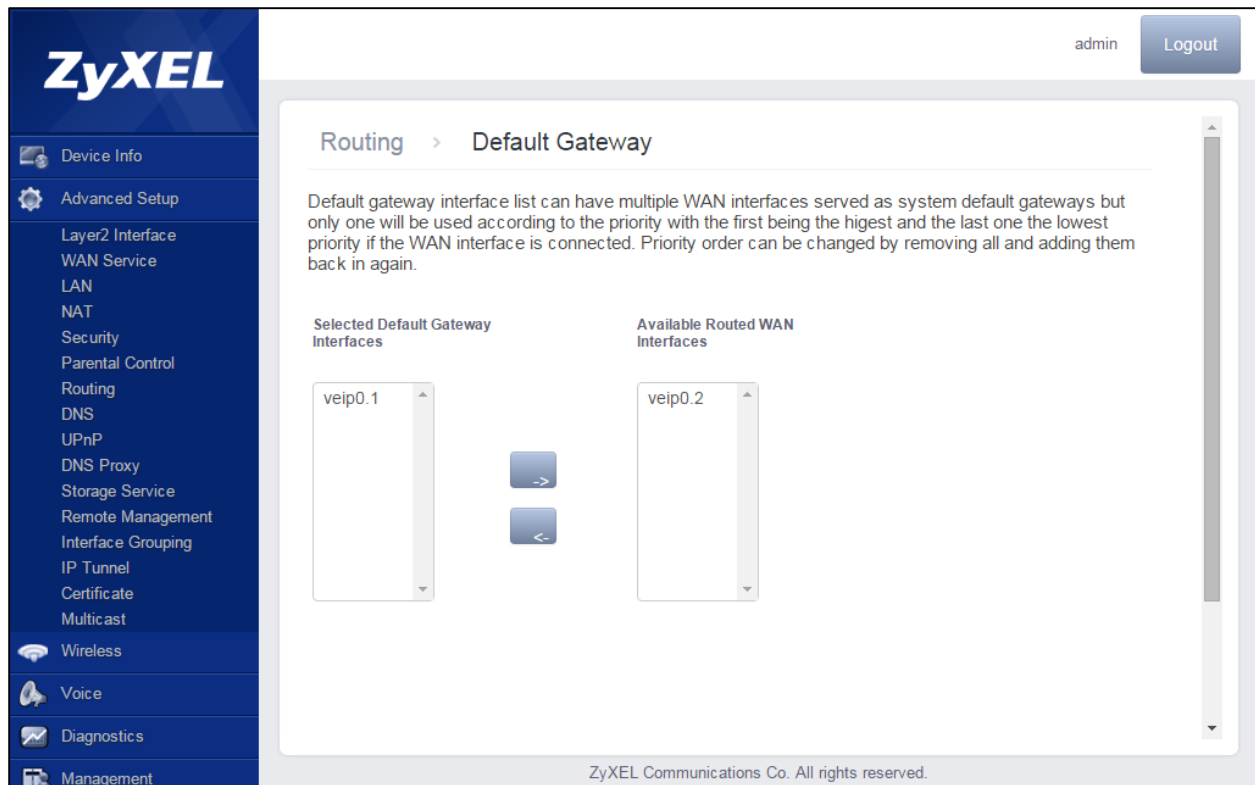


For the VoIP purpose, it is not required to enable the NAT service. Therefore we will only click next.

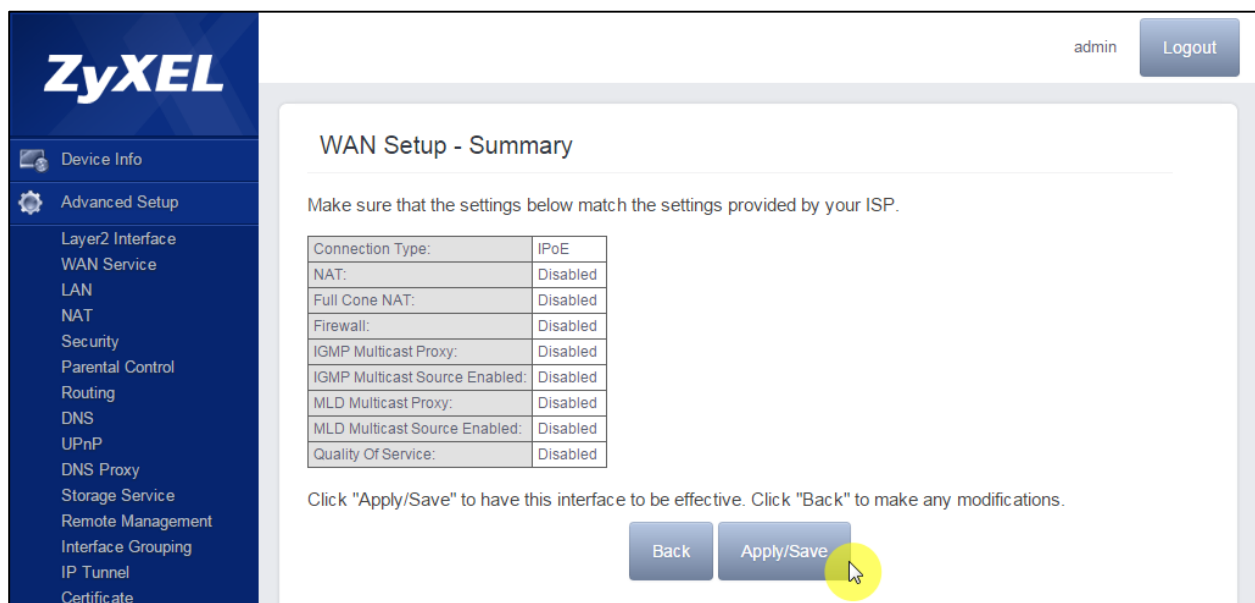


For the Default Gateway and DNS Server Configuration, we will not make any changes and only click on next for this two screens.





The WAN Setup summary will show us the overall setup, click on Apply/Save to store all changes.



The new WAN service will be displayed as follow:

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mid Proxy	Mid Source	Remove	Edit
veip0.1	data.100	IPoE	0	100	0x0	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
veip0.2	VoIP.200	IPoE	0	200	0x0	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

To Setup the Voice Service go to **Voice > Sip Basic Settings > Global Parameters** and select from the drop down box, the veip0.2 voice WAN service is selected in the Bound Interface Name.

To Setup the Voice Service go to **Voice > Sip Basic Settings > Service Provider 0**.

Select the Locale according to your regional settings.

Set the SIP server configuration according to your service provider specifications.

Enable the sip account.

Enter the sip account details according to your sip provider specifications.

Select the physical port number to which the line will be assigned.

Complete the procedure by clicking on Apply.

Global parameters **Service Provider 0**

Voice -- SIP configuration

Locale selection : USA - NORTHAMERICA

SIP domain name : 192.168.20.100

VoIP Dialplan Setting: x.T

Use SIP Proxy.

SIP Proxy: 192.168.20.100

SIP Proxy port: 5060

Use SIP Outbound Proxy.

SIP Outbound Proxy: 192.168.20.100

SIP Outbound Proxy port: 5060

Use SIP Registrar.

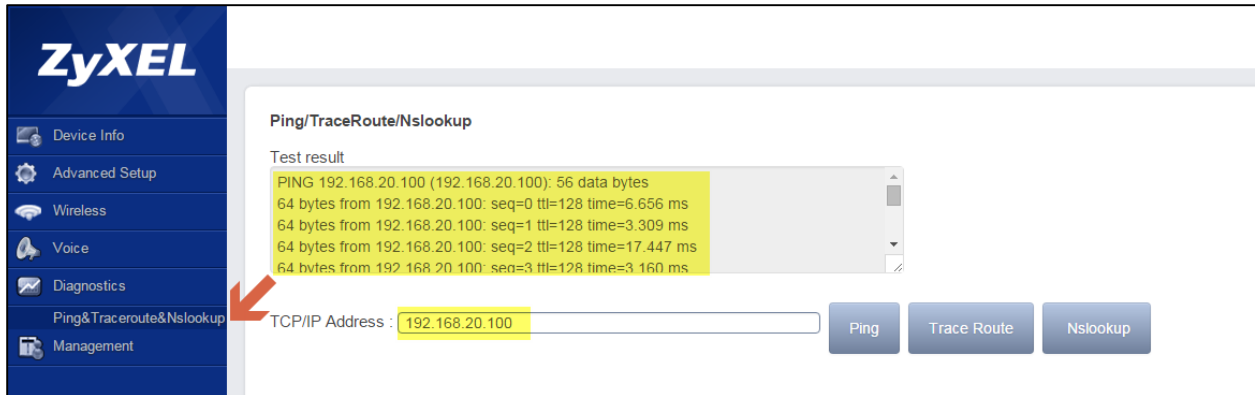
SIP Registrar: 192.168.20.100

SIP Registrar port: 5060

SIP Account	0	1
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Extension	101	102
Display name	Line 101	Line 102
Authentication name	101	102
Password	pass101	pass102
Physical Terminal Assignment	<input checked="" type="checkbox"/> Phone 1 <input type="checkbox"/> Phone 2	<input type="checkbox"/> Phone 1 <input checked="" type="checkbox"/> Phone 2
Preferred ptime	20	20
Preferred codec 1	G.711MuLaw	G.711MuLaw
Preferred codec 2	G.711ALaw	G.711ALaw
Preferred codec 3	G.723.1	G.723.1
Preferred codec 4	G.726_24	G.726_24
Preferred codec 5	G.726_32	G.726_32
Preferred codec 6	None	None

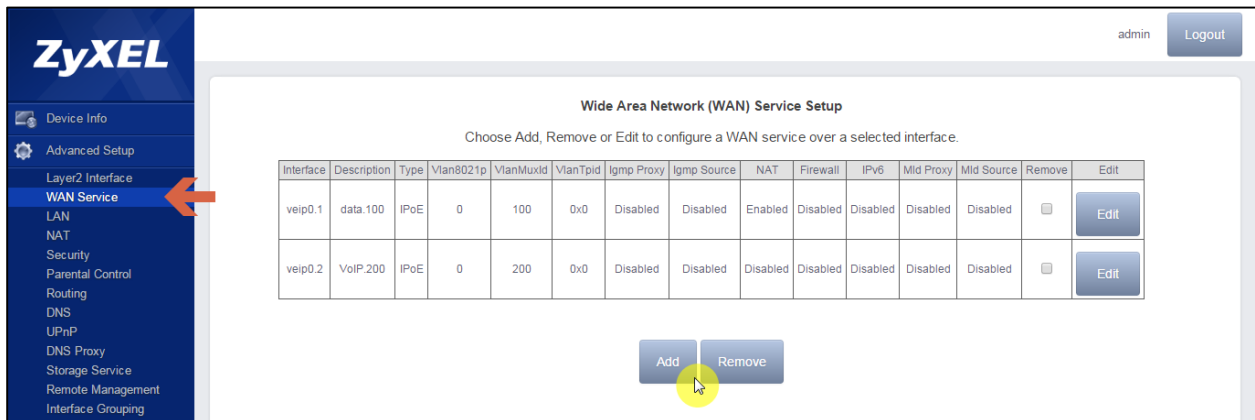
Apply

Similar to the data service it is possible to verify the ping diagnostic towards the sip server by going to **Diagnostics > Ping & Traceroute & Nslookup**.

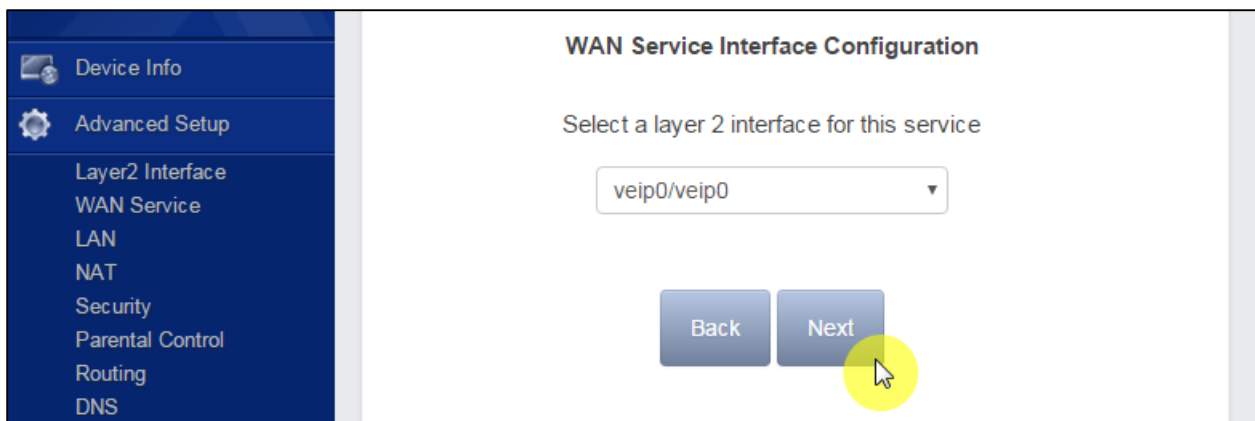


IPTV Service Setup

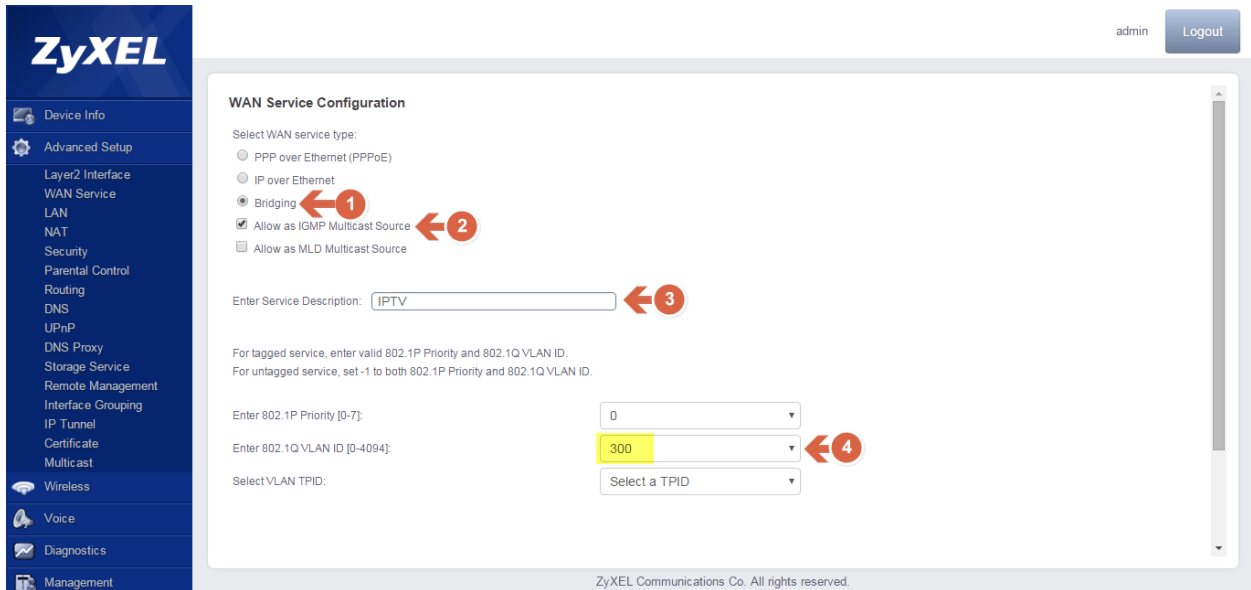
Go to **Advanced Setup > WAN Service** and click Add to create a new WAN Service.



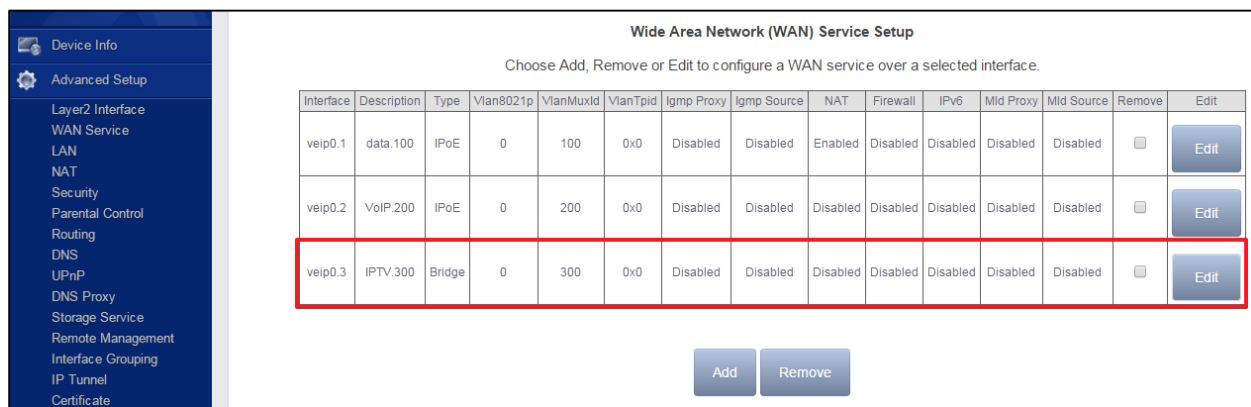
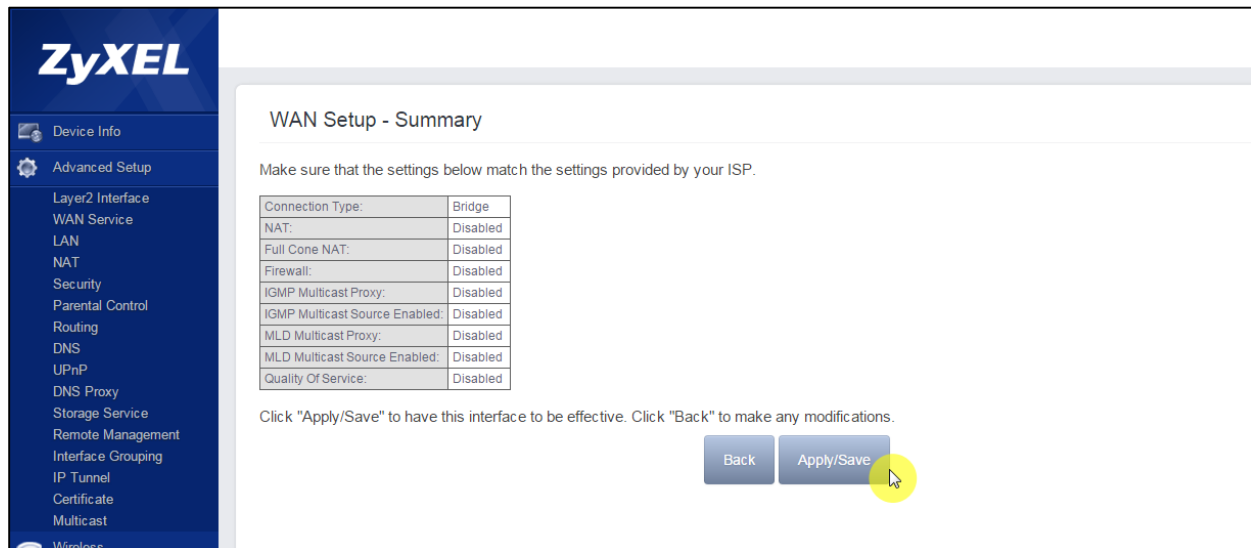
Click on next on when asked to select the layer 2 interface.



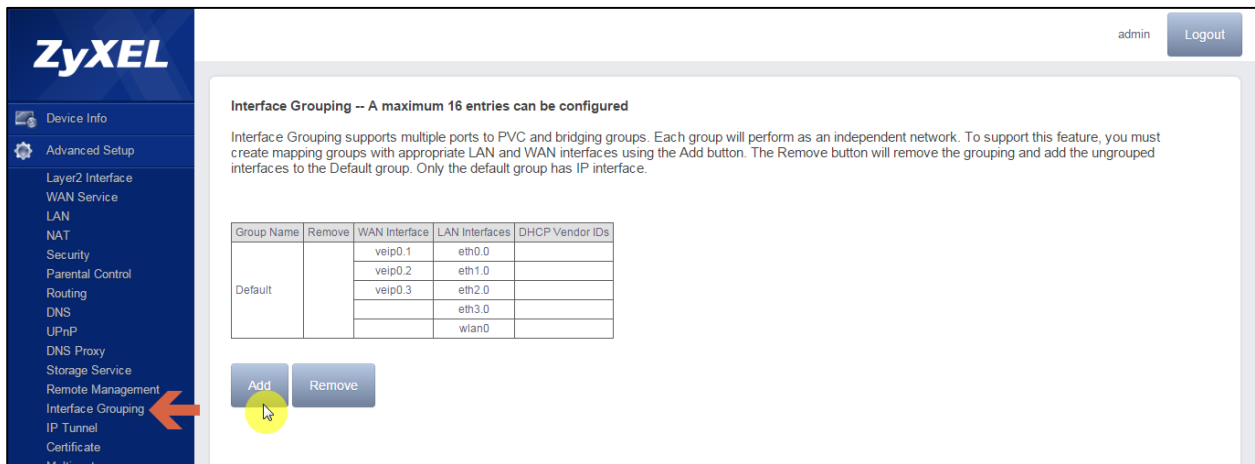
Setup the service type to Bridging and allow as IGMP multicast source. Then, optionally enter the service description. Finally, proceed to select the VID for the IPTV service in this example (VID 300). Proceed to click Next.



You will be prompted to the Summary screen to review all changed. Click Apply/Save to store the changes and finalize the service wan setup.

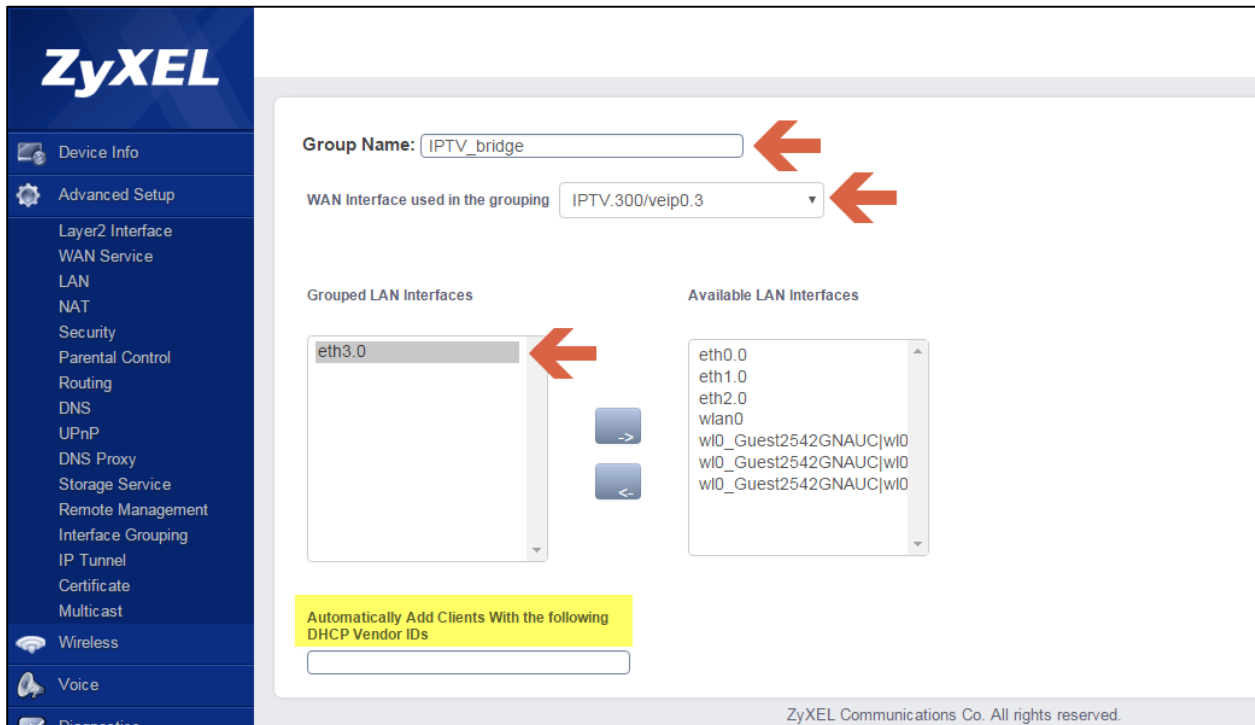


Go to Advanced Setup > Interface Grouping and click on Add to create a new interface.

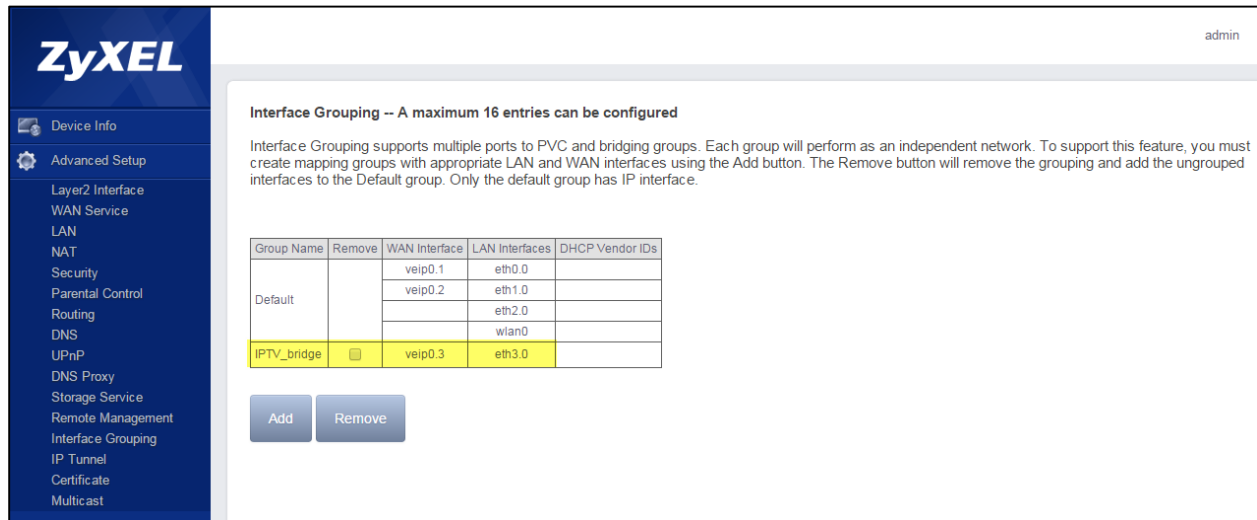


To create a bridge for IPTV, you can choose between statically selecting a port or automatically associate the LAN interface for bridge using the DHCP vendor ID. In this example, we have statically set port eth3.0, which is a reference to LAN port 4.

Start by defining the Group Name, then select the WAN Interface from the drop down box we previously created for the IPTV service. Select the desired port from the Available LAN interfaces and using the arrows to move to Grouped LAN interfaces. Complete the procedure by clicking the Apply/Save button.

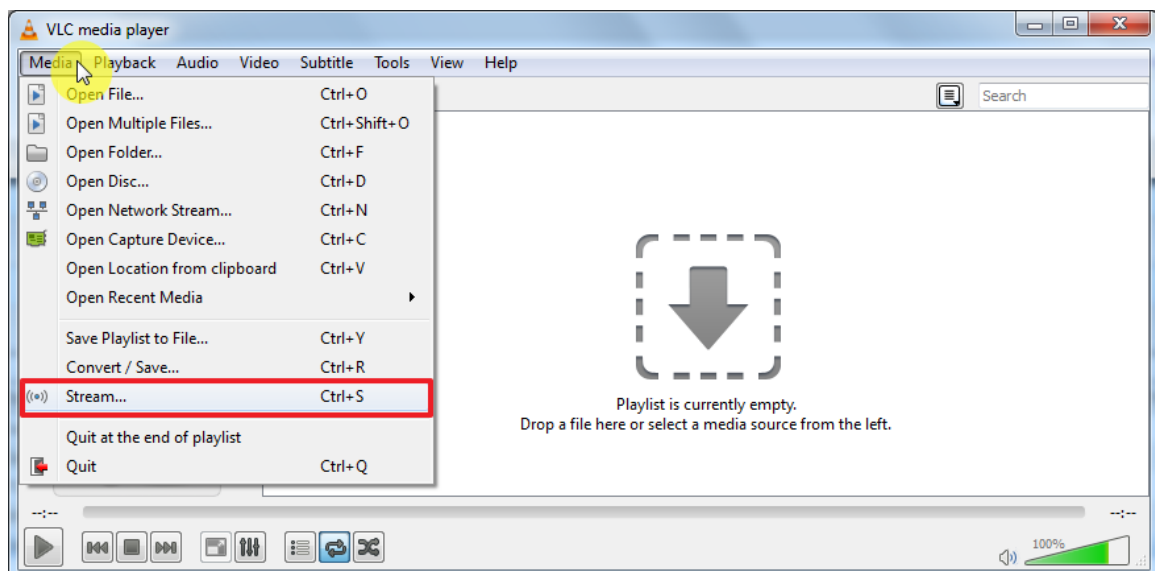


The bridge interface will now show up:

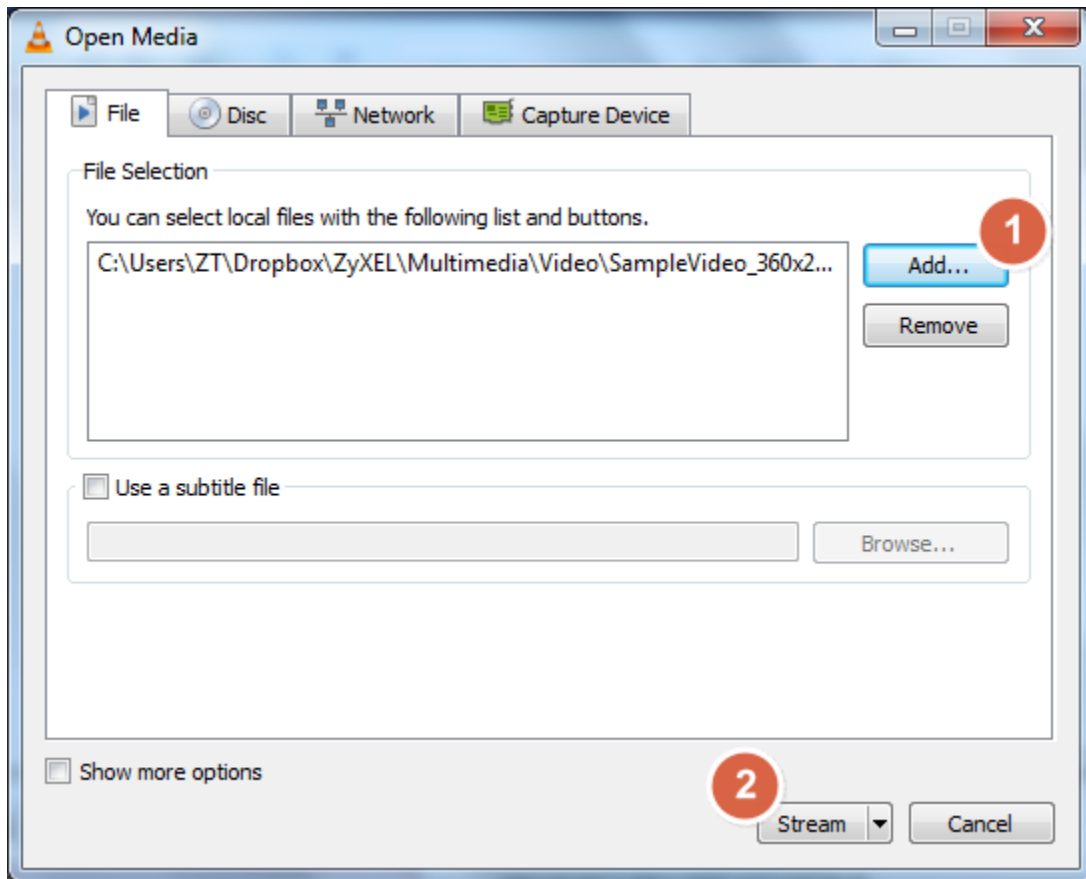


Test IPTV Bridge using VLC

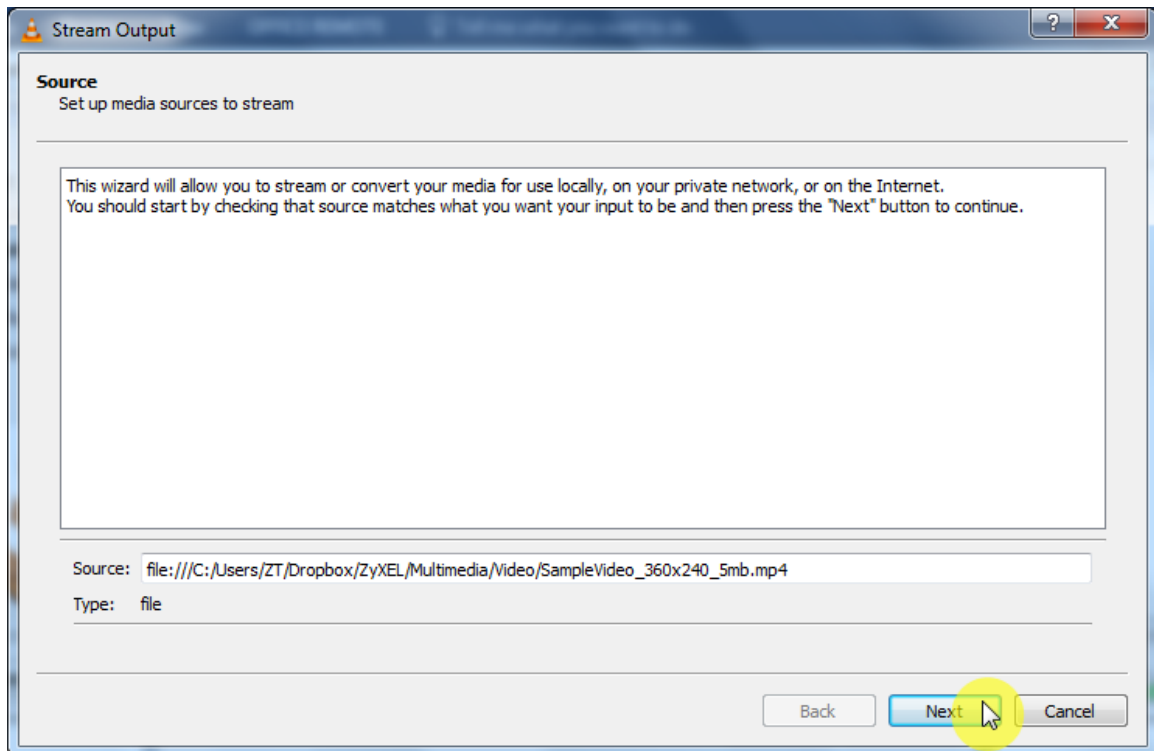
1. Connect a PC to the access port (untagged port) of the switch member of VLAN 300.
2. Run VLC program.
3. Go to Media > Stream... (May vary according to the version or operating system)



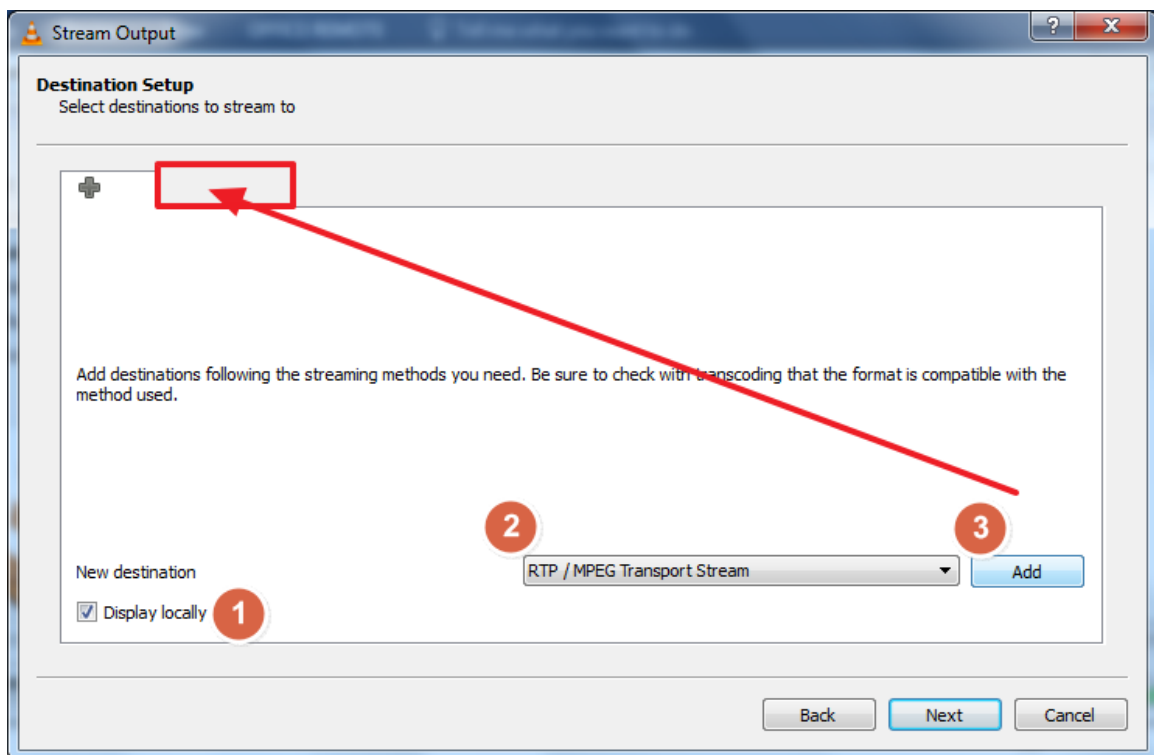
4. A new screen will pop-up, click Add to select a video file from your PC. Then, click stream.



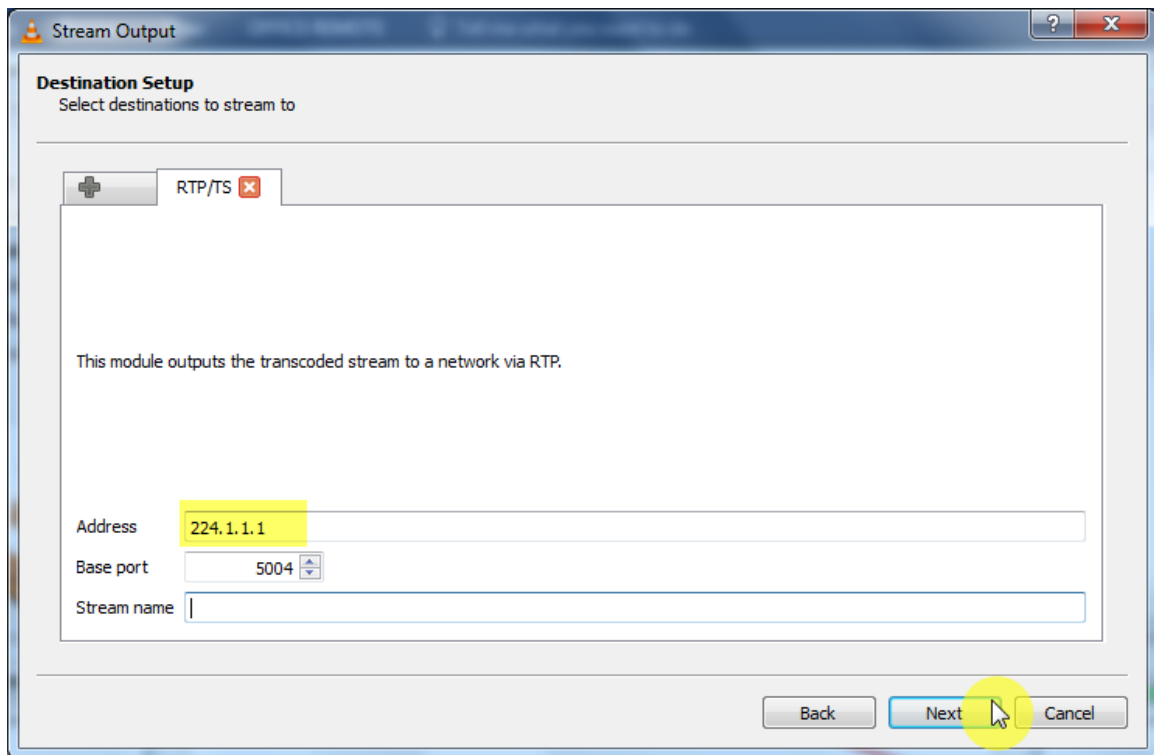
5. Click next on the following screen.



6. Click on the display locally, then choose RTP / MPEG Transport Stream from the drop down menu, then click add. This will add a new tab, click on the new tab.

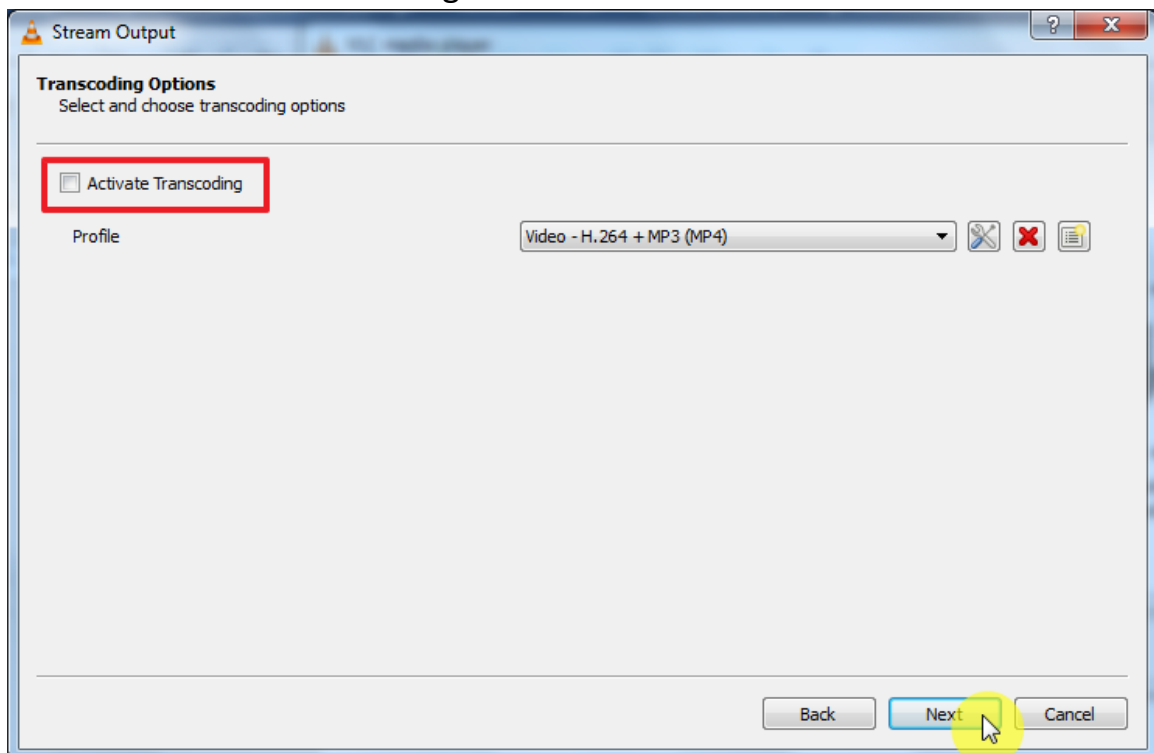


7. Input the multicast address, for this example 224.1.1.1, and click next to continue.



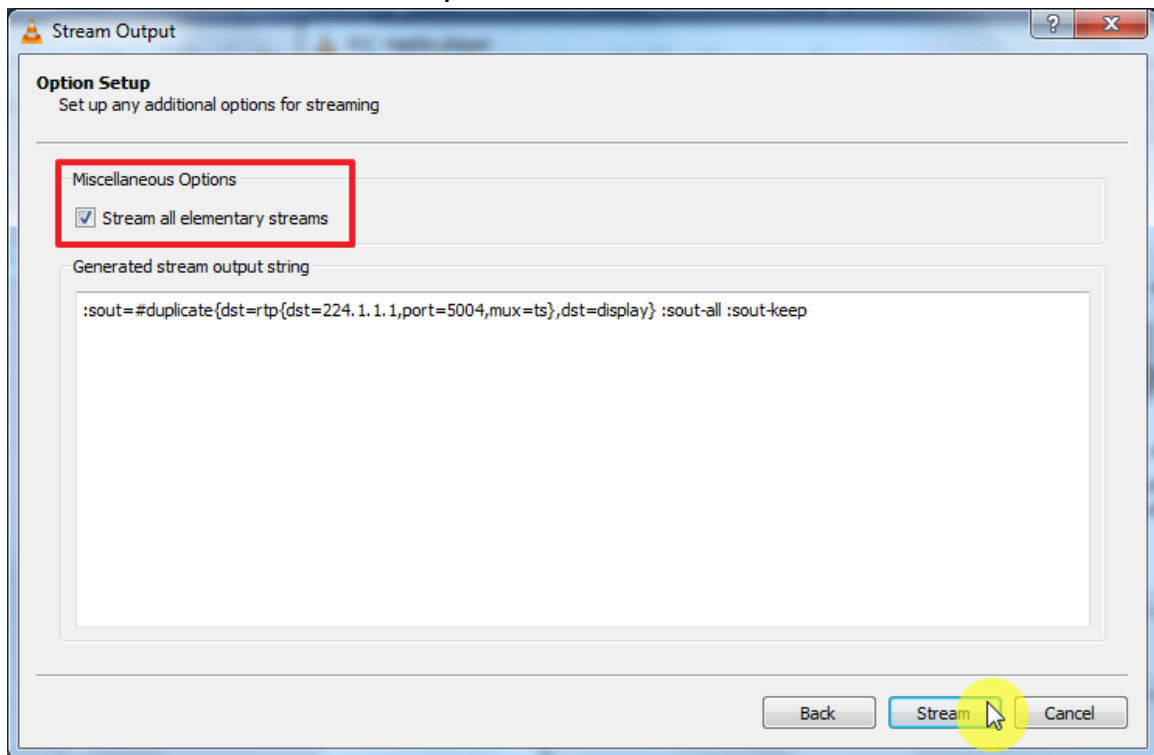
The screenshot shows the "Stream Output" dialog box with the "Destination Setup" tab selected. The dialog is titled "Stream Output" and has a subtitle "Select destinations to stream to". There is a tab labeled "RTP/TS" with a plus sign on the left and a close button on the right. Below the tab, there is a text area that says "This module outputs the transcoded stream to a network via RTP." Below the text area, there are three input fields: "Address" with the value "224.1.1.1", "Base port" with the value "5004", and "Stream name" which is empty. At the bottom right, there are three buttons: "Back", "Next", and "Cancel". A yellow circle highlights the "Next" button.

8. Clear the activate transcoding box and click next.

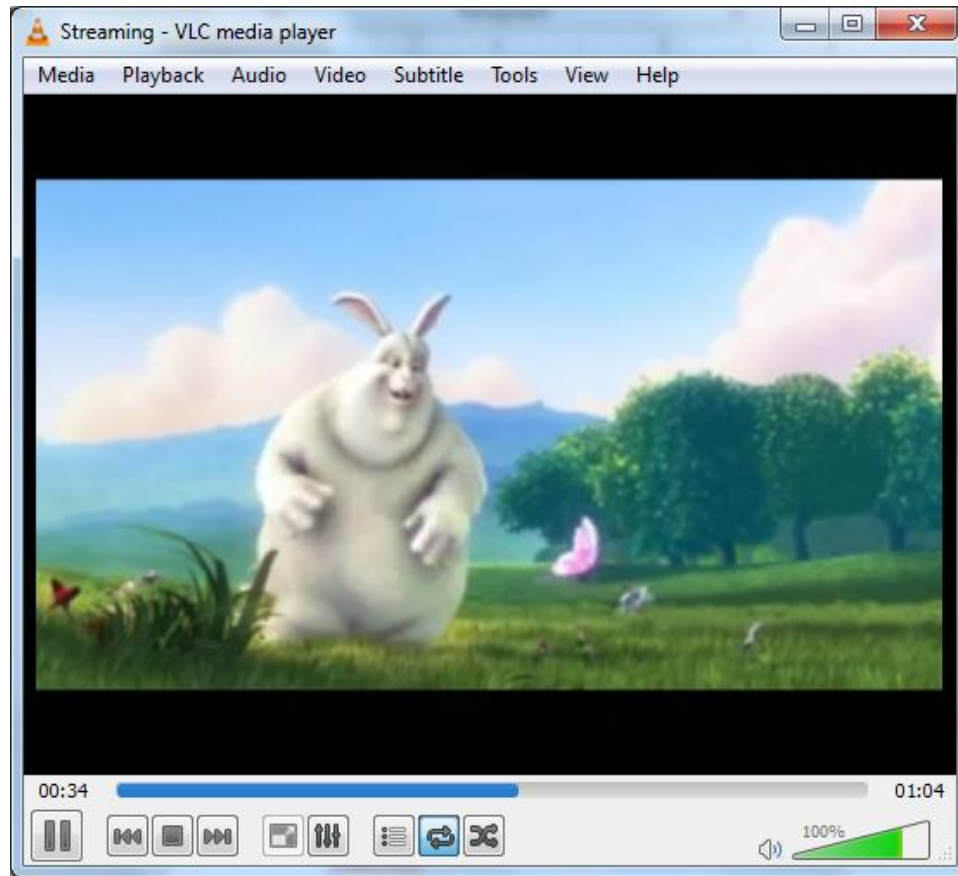


The screenshot shows the "Stream Output" dialog box with the "Transcoding Options" tab selected. The dialog is titled "Stream Output" and has a subtitle "Select and choose transcoding options". There is a checkbox labeled "Activate Transcoding" which is currently unchecked and highlighted with a red rectangle. Below the checkbox, there is a "Profile" dropdown menu with the value "Video - H.264 + MP3 (MP4)". To the right of the dropdown menu are three icons: a wrench and screwdriver, a red 'X', and a document icon. At the bottom right, there are three buttons: "Back", "Next", and "Cancel". A yellow circle highlights the "Next" button.

9. Select “Stream all elementary streams” and click Stream.



10. The VLC player window will show running the sample video.



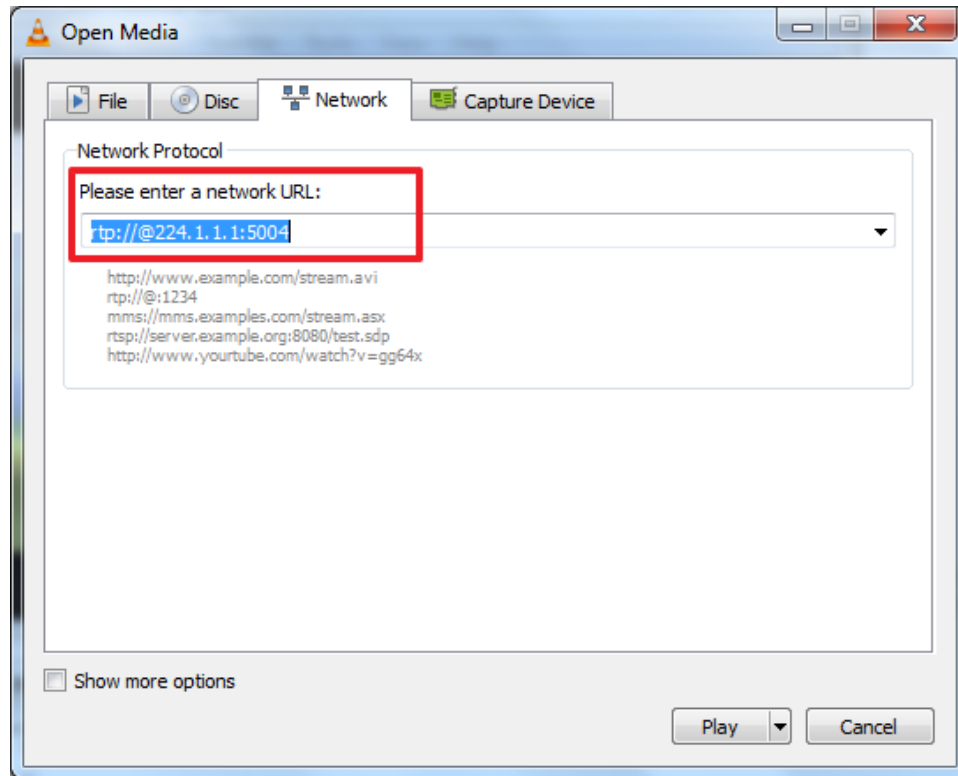
11. Using a network packet capture, we will be able to verify the IGMP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
115	18...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
117	18...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
118	18...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
121	18...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
124	18...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
169	19...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
193	20...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
203	20...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
232	20...	192.168.30.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources

▶ Frame 115: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 ▶ Ethernet II, Src: AsixElec_8e:c5:76 (00:0e:c6:8e:c5:76), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
 ▶ Internet Protocol Version 4, Src: 192.168.30.100, Dst: 224.0.0.22
 ▶ Internet Group Management Protocol

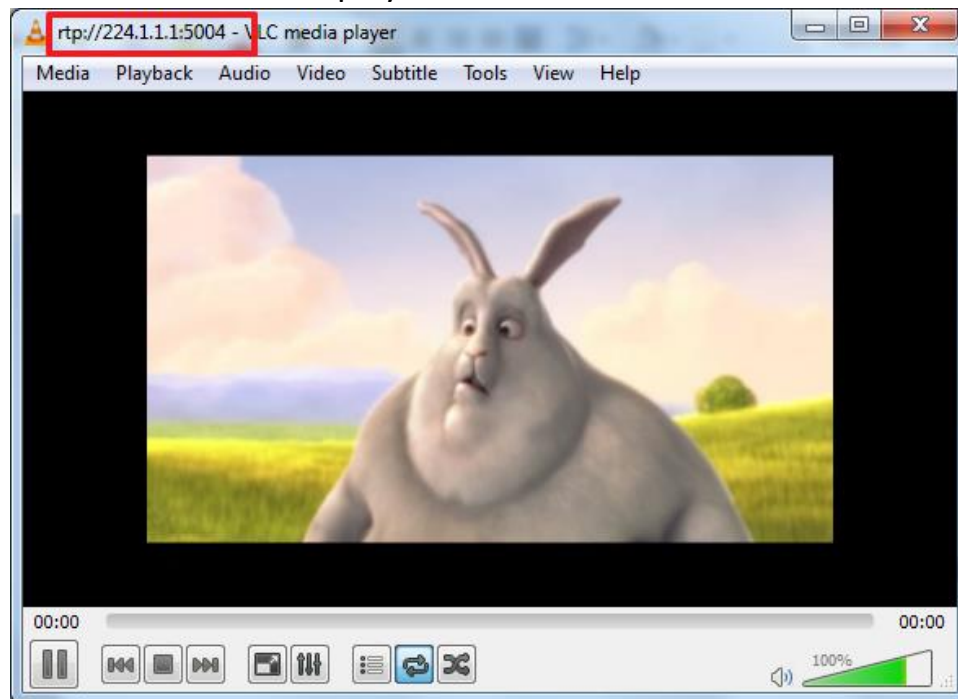
12. Now, connect a PC to the LAN port 4 (IPTV bridge) of the ONT and open VLC.

13. Go to Media > Open Network Stream



14. Enter the network URL as rtp://@224.1.1.1:5004 or rtp://224.1.1.1:5004.

15. The VLC stream will now display the video



Frequently Asked Questions

General Questions

- 1. What is the difference between the router and bridge modes supported by the GPON device?**

When the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use bridge mode which works similar to a switch to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet. For most Internet users having multiple computers want to share an Internet account for Internet access, they have to add another Internet sharing device, like a router. In this case, we use the router mode which works as a general router plus an Optical Network Terminal.

- 2. How do I know I am using PPPoE?**

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the PMG5318-B20B GPON device if the ISP uses PPPoE.

- 3. Why does my provider use PPPoE?**

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

Device Info Tab

Hardware

1. How to interpret the Power LED indications?

- The LED will turn steady green when ready for use or blinking green when self-testing.
- The LED will turn red when an error is detected, you may try rebooting the device to clear this status.
- The LED will be off when the GPON device is not turned on.

2. How to interpret the PON LED indications?

- The LED will turn steady green when it has a PON line connection or blinking green when downloading firmware.
- The LED will turn orange when the device has a fiber connected to the OLT but is not provisioned.
- The LED will turn red when no PON connection is detected or fiber is disconnected.
- The LED will be off when the PON link has been lost.

3. How to interpret the Internet LED indications?

- The LED will be steady green when it has an Internet connection but no traffic or blinking green when sending or receiving IP traffic.
- The LED will be red when it attempted to get an IP address but failed to receive it.
- The LED will be off when no IP connection is detected.

4. How to interpret the USB LED indications?

- The LED will be steady green when it has recognized a USB connection for its corresponding port or it will be blinking green when sending or receiving traffic through its respective USB port.
- The LED will be off when no USB has been detected on the corresponding port.

5. How to interpret the Ethernet LED indications?

- The LED will be steady green when a device is connected to the corresponding port or blinking green when IP traffic is passing through the corresponding LAN port.
- The LED will be off when no IP connection is detected through the corresponding LAN port.

6. How to interpret the Phone LED indications?

- The LED will be steady green when a SIP account is registered to the corresponding phone port, or blinking green when the telephone is off hook or has an incoming call.
- The LED will be steady amber to indicate a voice mail or blinking amber when the telephone is off hook with a voice mail, or a call is incoming and there is a voice mail for the corresponding line.
- The LED will be off when no SIP account is registered.

7. How to interpret the Wi-Fi LED indications?

- The LED will be steady green when the wireless network is activated, or blinking green when communicating with other wireless devices.
- The LED will be blinking amber when the GPON device is setting up a WPS connection.
- The LED will be off when the wireless network has been deactivated.

8. What is the WLAN button used for?

The WLAN button will power on or off the wireless local area network (WLAN) after being pressed for one second.

9. What is the WPS?

Typically to connect a wireless device to a router you need to know the router name (SSID) and its password. Wi-Fi protected support (WPS) is used to create network connections between the wireless router and the wireless devices quickly and securely.

10. What to do in case you forget the GPON device password?

You can press the reset button at the back of the device for more than 5 seconds in order to reload the factory configuration, meaning all the pre-configured settings will be erased from the device.

Summary

1. How can I access the Web GUI?

You can access the web configurator using a web browser and the device IP address. The user name "admin" has unrestricted access to change and view configuration of your Broadband Router. The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software. By default, the password for this user names are "1234".

2. What is the difference between the device serial number and the GPON serial number?

The GPON serial number is used by the device for its GPON connection with the OLT. The device serial number is an identifier of the physical hardware.

3. What is the Build Time Stamp?

The build time stamp identifies the firmware release date in the format YYMMDD_HHMM.

4. Why are there two software version?

The ONT can hold up to two firmware simultaneously, one being the active firmware running on the device, and the other a standby firmware.

5. What is the uptime?

The uptime displays how long the ONT has been running since it's last boot up.

6. What is the LAN IPv4 address?

An Internet Protocol version 4 address is a label assigned to each device using the IP protocol in a network to identify each participating device. The address is usually represented in a dot decimal notation, for example 192.168.1.1 will be the factory default address of the LAN for the GPON device.

7. What is the MAC Address?

The MAC (Media Access Control), also known as physical address, is used to identify each network interface to communicate in a network segment. The

mac address of a device is usually displayed in hexadecimal format, for example: 01:23:45:67:89:10.

8. What is a DNS Server?

The Domain Name Server maps a domain name to its corresponding IP address and vice versa. The DNS server enables ease of navigation for user, as instead of remembering several IP addresses, it is only necessary to write the domain name in your favorite web browser.

9. What is the safe temperature range for the optical transceiver operation?

The safe range is from 0 to 70 Celsius degrees.

10. What is the safe voltage range for the optical transceiver operation?

The safe range is from 3.13 to 3.14 volts.

11. What is the Bias current and what is the safe operation range?

The bias current is the specific current at specific measured point required for the proper device operation. The safe range for the bias current is from 4 to 50 mA.

12. What is the safe optical Rx power range of operation?

The safe range is from -28 to -8dBm.

WAN

1. Where can I find my WAN interface details?

Go to Device Info > WAN, this tab contains the information related to all WAN interfaces created in the GPON device:

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address
veip0.1	Data.100	IPoE	100	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Connected	192.168.10.6	
veip0.2	VoIP.200	IPoE	200	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	192.168.20.5	
veip0.3	IPTV.300	Bridge	300	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0	
veip0.4	MGMT.2302	IPoE	2302	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.16.1.201	

This table provide an overview of each interface for quick troubleshooting or identifying the settings originally defined for an interface.

A WAN may have defined multiple interfaces which are identified by the name of the managed element in this case VEIPO which identifies the Virtual Ethernet Card (Router mode) for this device, followed by the index number of the interface. In this table, it is possible to identify key information like the encapsulation type (IPoE, PPPoE, or Bridge), as well as the VLAN ID, status of the interface and IPv4 address among other relevant details. This information will let you verify the correct settings are defined for a specific interface.

Statistics

1. How to read the LAN and WAN statistics?

The LAN and WAN statistics provide valuable information about the network traffic passing through each LAN port or WAN interface. Both tables provide details on the amount of bytes and packets that pass through each interfaces showing additional details to detect potential issue like errored or dropped packets per interface, or a classification of the packets as multicast, unicast or broadcast.

Statistics -- WAN																	
Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.1	Data.100	80716566	687456	0	0	0	0	687455	1	1146092334	1303201	0	0	0	0	1303201	0
veip0.2	VoIP.200	399653	4811	0	0	0	0	2	4809	1522	5	0	0	0	0	5	0
veip0.3	IPTV.300	418214	5012	0	0	0	0	0	5012	4036	48	0	0	0	0	46	2
veip0.4	MGMT.2302	940846	9346	0	0	57240	795	3304	5247	3297793	4319	0	0	0	0	4319	0

Statistics > LAN																	
Interface	Received								Transmitted								
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast	
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	
eth0	1141480129	1307015	0	0	0	531	1306484	0	94664867	684941	0	0	0	1958	682983	0	
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
wl0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	1	

In order to troubleshoot issues, it is possible to reset the counters in order to create a closed timeframe for a set of statistics.

Route

1. What is a routing table?

The routing table contains a set of rules, which are often defined in a table format determining the destination of the packets in IP protocol.

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	192.168.10.1	0.0.0.0	UG	0	Data.100	veip0.1
172.16.1.0	0.0.0.0	255.255.255.0	U	0	MGMT.2302	veip0.4
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.2.0	0.0.0.0	255.255.255.0	U	0		br1
192.168.10.0	0.0.0.0	255.255.255.0	U	0	Data.100	veip0.1
192.168.20.0	0.0.0.0	255.255.255.0	U	0	VoIP.200	veip0.2

The destination represents the IP address to which the entry applies, the gateway defines where the GPON device sends the traffic. The Subnet Mask identifies the mask of the destination set and the flag marks the current state or characteristics of this entry. The service identifies the interface name to which a specific route applies and the interface identifies the specific entry to send the traffic through.

ARP

1. What is ARP?

ARP stands for Address Resolution Protocol. It is a protocol used to map network addresses to physical address.

2. What is an ARP table and how to read it?

An ARP table is maintained by the GPON device to map network addresses and physical addresses. It is used to identify the MAC address to the physical address and to its associated interface shown in the device column.

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.10.1	Complete	08:00:27:00:00:00	veip0.1
172.16.1.100	Complete	00:00:00:00:00:00	veip0.4
192.168.1.2	Incomplete	00:00:00:00:00:00	br0

DHCP

1. What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol and it provides the IP addresses to IP hosts in a network segment. It is useful to prevent the overhead of association a mac address with its respective IP address device per device. It may also provide additional information required for a specific network related configuration.

2. How to read the DHCP Lease table?

The DHCP lease table provides a mapping of IP addresses to physical addresses. It also provides the hostname of the device and the expiration term for the IP address assignment.

Device Info > DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
EDV8	08:00:27:00:00:00	192.168.1.2	21 hours, 1 minutes, 15 seconds

Advanced Setup Tab

Layer 2 Interface

1. What is Layer 2?

The layer two in the OSI model identifies the Data Link Layer. In this layer we can define a link between directly connected devices. The MAC address is mainly used to identify and handle devices at this level. In case of the GPON device we will create a GPON interface for layer 2 to communicate with the network.

WAN Service

1. What is a WAN?

A WAN is a set or collection of networking devices spread over a geographic area. A WAN is usually defined by an ISP to provide services to a specific area and for specific services, like Internet, VoIP or IPTV.

NAT

1. What is the difference between Virtual Servers, Port Triggering and DMZ host?

Virtual servers allow to redirect the IP traffic incoming from the WAN side to a private address on the LAN side. For example, a PC running a game as a

server can be accessed from outside the LAN using this method. Port triggering allows specific ports to be opened in the router firewall to be accessed by third parties, for example an FTP connection incoming from the WAN. Finally, a DMZ host will redirect all traffic to a host at a defined IP address. This host will have all ports opened, and traffic that has not been explicitly directed to a virtual server will end at this host, which usually is a firewall device or another NAT service.

Security

1. What is the difference between IP filtering and MAC Filtering?

IP filtering enables to block IPv4 or IPv6 outgoing traffic by filtering per protocol, by source IP, source port, destination IP, and/or destination port. A combination of several filters is allowed, and for the filtering to occur all set filters must be satisfied.

2. How to setup IP filtering?

To setup IP filtering go to Advanced Setup > Security > IP Filtering and click on the add button to add a new filter. A new screen will be displayed showing all the available filter options. For example, to block ICMP traffic a specific IP address you may setup IP version as IPv4, then protocol as ICMP and destination IP address you want to block.

3. How to setup Mac filtering?

The MAC filter may only be configured for interfaces defined as bridge and may block traffic by protocol type (e.g. IGMP), destination MAC address, and/or source MAC address. A combination of this filters may be applied as well as the direction in which the traffic is blocked (e.g. from LAN to WAN).

Parental Control

1. What is Parental Control?

Parental control enables the setting of restrictions to specified devices connected to the LAN. This restriction may be set by time or by URL.

2. How to setup parental control?

To setup parental control to restrict the traffic of a device connected to the LAN input the MAC address of the PC to restrict access, set the days for the restriction and the start and end time.

User Name	<input type="text" value="ChildrenTime"/>						
<input type="radio"/> PC MAC Address	<input type="text"/>						
<input checked="" type="radio"/> Custom MAC Address (xx:xx:xx:xx:xx:xx)	<input type="text" value="80:49:71:0f:91:fa"/>						
Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Start Blocking Time (hh:mm)	<input type="text" value="00:00"/>						
End Blocking Time (hh:mm)	<input type="text" value="20:00"/>						

Make sure you have set the modem time in Management/Internet time before setting the restrictions. Multiple restrictions can be set to define several different time frames.

Restriction can be defined by URL as well, two types of URL restrictions may be defined, Exclude and Include. If you define the exclude option, this will block the access to the URLs you define in the list. If include option is set, then it will only allow access to the URLs defined in the list.

Routing

1. What is a default gateway?

The default gateway is the node that will route packets to other networks. The default gateway is the generic route to which packets without a specific route in the routing table are sent to. For example, in the home router, the Internet WAN service will be defined as the default gateway to connect to hosts or websites in external networks. In the GPON device configuration the default gateway may be defined when creating the Internet WAN interface or later modified by accessing Advanced Setup > Routing > Default Gateway and selecting the WAN Interface to serve as the system's default gateway.

2. What is a static route?

Static route is a manually configured route defined in the routing table, rather than dynamically set. As these are static (fixed) routes they remain even after network changes, unless manually reconfigured. Static routes prove to be useful when defining a link between a few devices to increase routing efficiency or to define a failsafe route in case the default gateway fails.

3. How to setup a static route?

You can define a static route by accessing the web GUI and clicking Advanced Setup > Routing > Static Route. There you will be able to add a new entry; there you will be presented with the screen where you will be able to setup the IP version between IPv4 or IPv6. Define the destination IP address and prefix length of the destination. Then select the interface to where the traffic will be sent. The metric is the cost of transmission, better routes (like

shortest paths, or less congested paths) should have lower cost of transmission.

4. In what cases is policy routing used?

Other than the traditional view of routing based on the destination address only and taking the shortest path to forward a packet, this conventional method employs the routing table to define the destination of a packet. It is possible to define a policy routing to consider other factors, which will in turn override the default routing behavior and alter the packet routing.

Policy based routing takes precedence to normal routing. And it can be used to direct traffic from different users through different connections or create load sharing.

5. How to setup policy routing?

Policy routing can be defined by clicking on Advanced Setup > Routing > Policy Routing which will display a screen that will enable us to set policies by defining the source IP and/or Port and setting the destination of packets as a WAN interface, which has to be previously configured in the WAN interface section.

6. What is RIP When should I use it?

RIP stands for Routing Information Protocol. RIP is a routing protocol that works by counting the hops from a source to destination as a measurement of its metric. It is used to prevent loops by setting a maximum number of hops. The protocol is repeatedly sending updates of the routing tables to its neighbors, which lately has been proven to be a disadvantage given the increase in size for network tables due to network growth and may create a significant load of network traffic.

DNS

1. What is DNS?

DNS stands for Domain Name Server. And its main function is to map human readable and generally more memorable address to their corresponding IP addresses. This system is what enables you to write a `www.somedomain.com` in the address bar of your favorite browser instead of remembering the IP address of each website you wish to visit. You may think of it as the address book in your phone, who remembers phone numbers any more, people search in their cellphones for the name of people and in turn the phone book will use the phone number to contact the person. It is the similar function for the DNS server, which will use the human readable address and in return use the computer readable address which in this case is the IP address of the website to access. The DNS server is generally automatically provided by the Internet Service Provider.

2. What is Dynamic DNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet.

To use the service, you must first apply an account from several free Web servers such as `http://www.noip.com/`. Without DDNS, we always tell the users to use the WAN IP of the GPON device to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the GPON device, you apply a DNS name (e.g., `www.zyxel.com.tw`) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the `www.zyxel.com.tw` regardless of the WAN IP of the GPON device.

When the ISP assigns the GPON device a new IP, the GPON device updates this IP to DDNS server so that the server can update its IP-to-DNS entry.

Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

It is possible to check IP address(es) for a URL by running a nslookup in the command prompt as follow:

```
C:\Users\ZT>nslookup www.google.com
Server: UnKnown
Address: 172.21.65.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4008:c06::93
           64.233.188.99
           64.233.188.147
           64.233.188.103
           64.233.188.106
           64.233.188.104
           64.233.188.105

C:\Users\ZT>_
```

In turn you may input the IP addresses directly to your web browser and be directed to the notorious search engine Google™.

1. When is DDNS needed?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the PMG5318-B20B GPON device sends this IP to the DDNS server for its updates.

3. What is UPnP?

UPnP stands for Universal Plug and Play. It is a distributed open networking standard that used TCP/IP simple peer-to-peer network connectivity between devices. A UPnP device can automatically join a network, obtain an IP address, convey its capabilities and learn about other devices on the

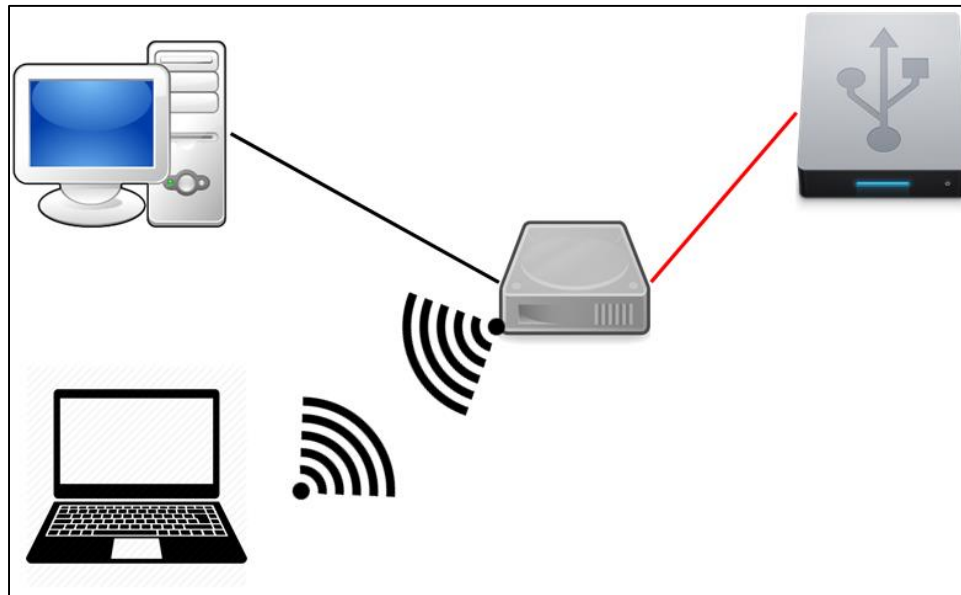
network. In turn, a device can leave a network smoothly and automatically when it's no longer in use.

UPnP devices are called plug and play because when this feature is enabled, the devices will announce their network address and available services, which will enable clients to immediately start using those services.

Storage Service

1. What is the storage service?

Using the on board file storage service you can connect a USB memory stick or hard drive to your GPON Device's USB with users on your network.



After connecting a USB device, you can check it by going to Advanced Setup > Storage Service > Storage Device Info.

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

➔

Volumename	FileSystem	Total Space	Used Space
disk1_1	fat	7712	7114

2. How to setup the user accounts?

In order to access the USB device, you will need to first setup a user account by going to Advanced Setup > Storage Service > User Accounts. There you will be presented with a screen to input the user name and password details.

3. How to access the USB connected to my PMG5318-B20B?

You can access a connected USB by using the windows explorer and connecting to the ONT IP like <\\192.168.1.1\share>.

Remote Management

1. How do I enable/disable Management from the WAN or LAN?

To enable remote management to access the ONT by the web GUI or command line for configuration, go to Advanced Setup > Remote Management. Click enable and select between the options for each type of service or protocol to enable the access by LAN, WAN, only a trusted domain or block all remote management access.

Remote management can be useful to provide quick access for the service provider to verify the GPON device configuration or provide remote assistance.

Wireless Tab

1. What is a wireless LAN?

Wireless LANs provide all the functionality of wired LANs, without the need for physical connections (wires). Data is modulated onto a radio frequency carrier and transmitted through the ether. The GPON device wireless LAN works in the 2.4GHz band and is compliant with IEEE 802.11b/g/n, using a 2x2 MIMO technology to reach up to 300Mbps PHY rate.

2. What is MIMO?

MIMO stands for Multiple Input Multiple Output. This technology enables wireless network to be speedier. It works by increasing the number of receiver and transmitter antennas. The additional antennas work together to provide better performance without increasing the bandwidth or requiring too much additional power.

3. What are the advantages of a WLAN?

- **Mobility:** Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation Speed and Simplicity:** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- **Installation Flexibility:** Wireless technology allows the network to go where wire cannot go.
- **Reduced Cost-of-Ownership:** While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- **Scalability:** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

4. What is a disadvantage of WLAN?

The speed of Wireless LAN is still relatively slower than wired LAN. The setup cost of Wireless LAN is relative high because the equipment cost including access point and PCMCIA Wireless LAN card is higher than hubs and CAT 5 cables.

5. What is an Access Point?

An access point (AP) is a wireless device that with an antenna and a wired Ethernet connection broadcasts information using radio signals. An AP typically acts as a bridge for the clients to extend the reach of a network. It can pass information to wireless LAN cards in PCs allowing those computers to connect wirelessly to a campus network for example.

6. Is it possible to use wireless products from a variety of vendors?

Yes. As long as the products comply with the standard IEEE 802.11 b/g/n. The Wi-Fi logo is used to define the 802.11 family compatible products.

7. What is Wi-Fi?

The Wi-Fi logo means that a product is interoperable with wireless networking equipment from other vendors. A Wi-Fi logo product has been tested and certified by the Wireless Ethernet Compatibility Alliance (WECA). The Socket Wireless Lan Card is Wi-Fi certified, and that means that it will work (interoperate) with any brand of Access Point that is also Wi-Fi certified.

8. What type of devices use the 2.4GHz band?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE 802.11b), cordless phones, wireless medical equipment and Bluetooth short range

wireless application, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

9. Does 802.11 interfere with Bluetooth devices?

Any time devices are operated in the same frequency band: there is potential interference. Both the 802.11b/g and Bluetooth devices occupy the same spectrum. But a Bluetooth device would not interfere with other 802.11 devices much more than another 802.11 device would interfere. While more collisions are possible with the introduction of a Bluetooth device, they are also possible with the introduction of another 802.11 device or a new 2.4 GHz cordless phone for that matter. But, Bluetooth devices are usually low-power, so the effects that a Bluetooth device may have on an 802.11 network, if any, aren't far-reaching.

10. Can radio signals pass through walls?

Transmitting through a wall is possible depending upon the material used in its construction. In general, metals and substances with higher water content do not allow radio waves to pass through. Metals reflect radio waves and concrete attenuates radio waves. The amount of attenuation suffered in passing through concrete will be a function of its thickness and amount of metal re-enforcement used.

11. What are the potential factors that may cause interference among WLAN products?

- a. Obstacles (walls, ceilings, furniture, etc.)
- b. Building materials (metal doors, aluminum studs, etc.)
- c. Electrical devices (microwaves, monitors, etc.)

12. How to overcome interference factors for WLAN products?

- a. Minimizing the number of walls and ceilings.
- b. Locate antennas for better reception.
- c. Keep WLAN products away of electrical appliances.
- d. Add additional access points.

13. Should I enable client Isolation for my Wi-Fi access point?

Wireless Isolation, sometimes called client isolation, is a setting on a wireless router. When this setting is enabled it prevents a computer that is connected to the network by a wireless connection from accessing computers and resources that are connected to the network by a wired connection. It will also prevent one wirelessly connected device from connecting to another wirelessly connected device. In essence Isolating that device on the wireless network.

This is used as a method of security so that you can provide both wired and wireless connection through the same network without opening up secured computers and resources to potentially unwanted visitors. This can be very helpful in businesses that have a wireless hotspot located in their lobby for example.

14. What is a SSID, should I hide it?

SSID stands for Service Set Identifier, in simpler words it is used to name a particular wireless network. The GPON device is able to define several SSID each with different characteristics. For example, you can define an SSID for your home network with a set of privileges and a network for guests with less privileges or increased security.

In case, you want increased security you can hide your network. In this fashion only people you want to add to your network will find it.

15. How does the wireless bridge operate in my PMG5318-B20B?

It is possible to create a wireless bridge to extend the range of a wireless network with other compatible devices. By enabling the remote bridge feature, you'll be allowing selected APs to establish a wireless bridge connection with the GPON device. It is also possible to scan for nearby devices to automatically select them and create a bridge. This functionality can also be disabled.

Diagnostics Tab

1. What does it mean that my eth0 (1,2, or 3) connection passed?

Using the convenient help link located next to each test result, it is possible to interpret the result. If the test is passed for the Ethernet port, it means that a device (e.g. computer) is connected to a LAN port and that it has a successful connection with the GPON device.

2. I have no computers connected to my GPON device via Wi-Fi, why is the LED green and why the test shows passed?

The green LED for Wi-Fi determines that a Wi-Fi connection is available from the GPON device and the Wi-Fi passed test shows that the connection is present. Even though devices are not connected to the Wi-Fi, it is possible to determine in this fashion that a connection is available and present for devices to readily connect.

3. What should I do if a test is failed for a LAN port or Wi-Fi connection?

The help link next to the test result, also provides insightful information about the troubleshooting when a test is failed.

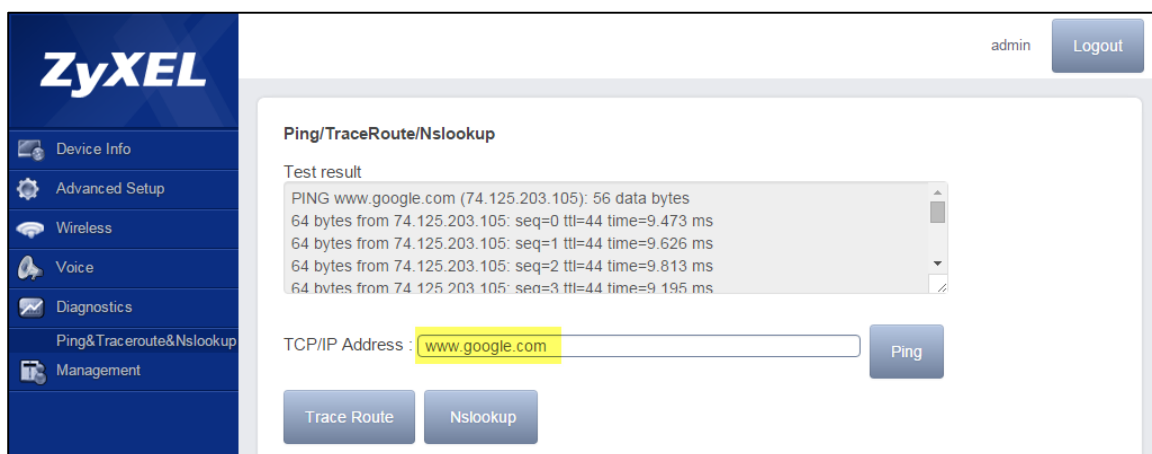
In case of the failure of a LAN port it is suggested to test:

- a. If you are not able to access this page, verify that the Ethernet cable from your computer or your hub is connected to the LAN port on the GPON Router. Reset the cable by unplugging both ends and reconnecting them to their respective ports.
- b. In case of a Wi-Fi connection issue, verify that the wireless configurations from your computer and your broadband router are matched and correct.
- c. Turn off the Broadband Router, wait 10 seconds and turn it back ON.
- d. Make sure you are using the Ethernet cable supplied with your GPON device.
- e. With the router on, press the reset button on the Broadband Router for at least five seconds and release it. This resets the Broadband Router to its default settings. Wait for the Broadband Router to initialize, then close and restart your Web browser. To reconfigure the router, type your GPON device account username and password.
- f. Rerun the Diagnostics test, to verify the results. In case, the tests fail again contact the ISP technical support.

4. What is a ping test? When and how should I run it?

A ping test is a method to verify connection with a network or to a specific IP address. Microsoft Windows as most operating systems has this tool integrated in their systems natively. In order to run a ping test directly from the GPON device you may access the web GUI > Diagnostics > Ping&TraceRoute&Nslookup and input an IP address or URL into the TCP/IP

Address and click Ping. It will process for a few seconds and display the results.

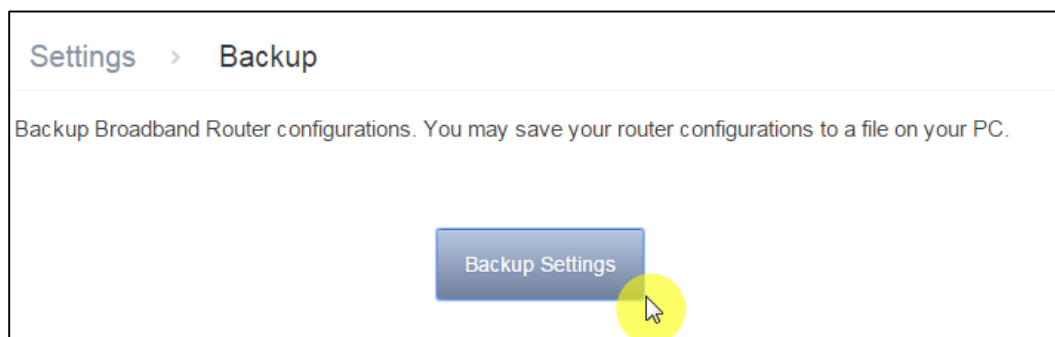


The Ping test should be run when required to test the network connection or to verify connectivity to a specific IP address.

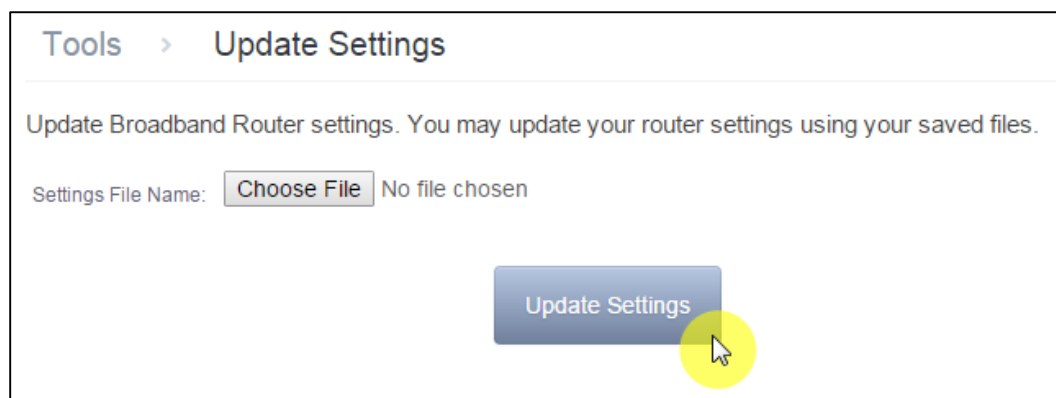
Management Tab

1. Why should I backup my ONT configuration and how to do it?

After the initial setup it is recommended to back up the configuration, in case it is later needed to reset the device to factory default, you may easily setup again all your service by restoring the file. It is possible to back up the configuration using the web GUI by accessing Management > Settings > Backup. There you will be presented with the Backup Settings button which will let you save the current device configuration to the local PC.



It is possible to restore or update the settings of the device by selecting the same file previously downloaded and accessing Management > Settings > Update. There you will be able to select the file and click on update settings to load the device configuration.



2. What is the difference between alerts and logs?

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as system errors consist of both logs and alerts. You may differentiate them by their color in the View Log screen. Alerts are displayed in red and logs in black.

3. How do I change the password to access the PMG5318-B20B web management?

It is possible to change the password of the device by accessing the Management > Access Control > Passwords. There you will be able to input the username for which you want to define the password and enter the old and new password for your device. Please remember to keep your password in a safe location. In case you forget the password to access your device a reset to factory default is required to access the device. The reset will cause all your configuration to be lost.

4. What is a software update?

A software update will be recommended by your ISP when new firmware is released for your device containing new features or improvements in performance. The software update must be done cautiously. Please verify that the firmware corresponds to the exact model of your device by checking the label at the bottom of your device. The upload of the firmware is done using the web GUI by locating at Management > Update Software. There you will be able to select the file, generally, with a bin file extension and click the Update Software button.

Tools > Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: No file chosen

5. What should I do if I forget the IP address of my GPON device?

The default IP address of your device is 192.168.1.1. In case you have changed the IP address and forgotten it, reset the GPON device by pressing the reset button for more than 5 seconds until the power LED begins to blink and then release it.

6. How to troubleshoot a failed internet connection?

Start by checking all cables are connected properly, and the LEDs are behaving as expected. For example, the PON LED will turn red if the optical connection has a malfunction or is not connected properly. Or will turn orange in case the device is not provisioned properly. In case the device is not properly provisioned contact your ISP for technical support.

Disconnect all cables of the devices for 10 seconds and reconnect. Make sure the WAN setup has been entered correctly and that the device is configured properly. It is possible to reset the device to factory default and try to input the information again to double check the configuration. In case the internet connection is not reestablished contact your ISP for technical support.