PON Madness - Bypass ISP XGS-PON ONT with…a stick?
Miguel R. - m@mig.sh

/// NOTICE ***///***

This document has now been deprecated and is now in legacy status. No new updates will be performed.

Documentation has been moved to https://pon.wiki

For AT&T, click *here*

For Bell, click

***here for Gigahub*,**

here for Home Hub 4000

Sidenote: Find us on the [8311 discord]

Product Technical Information

Product P/N from ECIN: EN-XGSFPP-OMAC-V2
Product Description from ECIN: XGS-PON ONT Stick v2 with MAC function mounted into a standard SFP+ package with local management based on Maxlinear chip

What it actually is: a rebadged BFW/Azores WAS-110 SFP+ transceiver
###

ECIN User Manual: XGS-PON_ONU_STICK-UserManual.pdf

End-User Management Routines

A WebUI can be found on https://192.168.11.1
Client device needs to be on same network as the management subnet, ex: 192.168.11.2/24

Credentials for the WebUI are:
Username: admin
Password: QsCg@7249#5281

(We've had some reports where telnet is disabled by default. Use the WebUI to enable it)

Technician Management Routines

A local shell is offered for technicians to be able to configure this ONU. To access this shell, configure your management device to an IP on the 192.168.11.0/24 network, like 192.168.11.2, then telnet on port 23 to 192.168.11.1 with the following credentials:

Username: `root`
Password: `QpZm@4246#5753`

Once logged in, you can reach the CLI by using *`load_cli factory`*.
Note: If you only type load_cli, it will ask for login, make sure to use the full command, load_cli factory.

First Setup Compatibility Warning: If the WAS-110 has no fiber PON connection, it **might not respond** at management IP 192.168.11.1 on certain NICs (Like the Intel E810-XXVDA4, Opnsense DEC3860, and Mellanox ConnectX-5) as they believe the link is down (returning RX loss), or they do not provide enough power (or the driver refuses to power it). Using a switch, like a Ubiquiti USW Pro Aggregation (or any other SFP+ capable switch) allows access to WAS-110 without the PON connection.

Bypass instructions for AT&T BGW320-500/BGW320-505

****/****/****/**** ATTENTION ****/****/****/****
These are the OMCI values extracted from the BGW320's encrypted config.cfg.
Do not use the ones listed on the Web UI.
****/****/****/**** ATTENTION ****/****/****/****

Gather the following information from the bottom of your BGW320:

[ ] Your ONT ID
[ ] Your MAC Address

Run the following commands in the `config\factorydir #` prompt after logging in and running *`load_cli factory`*

```
set factorymode enable
set device_sn HUMAXXXXXXXX
```
(or `NOKA` for the 505)

`set gpon_sn HUMAXXXXXXXX` (or `NOKA` for the 505)
`set vendor_id HUMA` (or `NOKA`, first 4 letters of ONT SN)
`show allinfo` (confirm new changes are correct before commiting)
`set factorymode disable`
`exit`

From here, this should drop you back to a root shell, run `sync` then `reboot` to reboot the ONU. To confirm your changes after the reboot, you can run `pon sng` to view the current PON serial number.

Some Notes: If you run *`pon sng`* before reboot, it will not reflect the changes, have *to run after reboot.* Also, **ensure you change your MAC address on your WAN port of your router to reflect the MAC from the RG.** If you don't do this you will experience slow speeds and poor stability for 20-ish minutes until the RG's DHCP lease with AT&T expires and probably freak out and cry on the Discord about how you aren't getting full speeds.

Bypass instructions for Bell

****/****/****/**** ATTENTION ****/****/****/****

THIS WILL BREAK SERVICE IF YOU HAVE TV OR PHONE SERVICE ON THE ACCOUNT.
ALSO, ENSURE YOU SETUP THE FAILSAFE! SET. IT. UP!

****/****/****/**** ATTENTION ****/****/****/****

Gather the following information from the bottom or side of your Bell-issued router:

- [ ] Your ONT ID
- [ ] Your MAC Address

FIRST: Set up the failsafe, found here. **Unless you do this, you will be permanently locked out of the device, and you will not be able to recover without a UART adapter.**

Once done, run the following commands in the `config\factorydir #` prompt after logging in and running *`load_cli factory`* *(You can ignore any errors when running this and factorymode enable commands)*

```
set factorymode enable
set device_sn SMBSXXXXXXXX (or ALCL/HWTC)
set gpon_sn SMBSXXXXXXXX (or ALCL/HWTC)
set vendor_id SMBS (or ALCL/HWTC)
show allinfo (confirm new changes are correct before commiting)
set factorymode disable
exit
```

Before you do anything else, check the failsafe is working by double checking the `# Confirm the change,` lines, ensuring they match expected outputs, and rebooting.
Once you run the next command, **you will lock yourself out**, and will need UART to recover unless failsafe is working.

```
uci set omci.default.mib_file=/etc/mibs/prx300_1V.ini; uci commit;
sync
```

On your router, ensure you're using vlan 35. If you are on Bell Canada (Not Aliant/MTS) start a PPPoE session.

CLI Command Listings

To switch between config types, use cd, as if you were changing directories.

User: user_commands.txt
Config: config_commands.txt
PON: pon_commands.txt
Device: device_commands.txt
Service: service_commands.txt
Factory: factory_commands.txt

Root Shell Listings

These are useful commands that exist in the linux environment, helpful for troubleshooting

Command	Description
`pontop`	A terminal user interface (TUI) that allows a user to look at all the PON protocol specifics, including GEM interfaces and statuses
`pon`	A command-line interface (CLI) that allows a user to use the PON libraries to get and view data from the PON chipset.
`i2c_cmd show optical`	This command allows you to view the optical data of the transceiver, as well as voltages and temperatures.
`omci_pipe.sh`	A command-line tool that allows a user to look at the MIB data coming in from a provider.

Known Working SFP Adapters

Mellanox ConnectX-4 Lx	NetXtreme II BCM57810	Intel X520-SA

Known Working Switches

Brocade ICX6610	Ubiquiti
Brocade ICX7450-32ZP	USW-Aggregation
	UDM-Pro

Appendix

Device Information

CPU Information

```
root@prx126-sfp-pon:/# cat /proc/cpuinfo
system type             : PRX300 rev 1.2
machine                 : PRX126-SFP-PON
processor               : 0
cpu model               : MIPS interAptiv (multi) V2.0
BogoMIPS                : 265.98
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : yes
hardware watchpoint     : yes, count: 4, address/irw mask: [0x0ffc,
0x0ffc, 0x0ffb, 0x0ffb]
isa                     : mips1 mips2 mips32r1 mips32r2
ASEs implemented        : dsp mt eva
Options implemented     : tlb tlbinv segments 4kex 4k_cache prefetch
mcheck ejtag llsc pindexed_dcache userlocal vint perf_cntr_intr_bit cdmm
nan_legacy nan_2008 ebase_wg perf
shadow register sets    : 1
kscratch registers      : 0
package                 : 0
core                    : 0
VPE                     : 0
VCED exceptions         : not available
```

```
VCEI exceptions          : not available
```

Memory Management Information

```
root@prx126-sfp-pon:/# free
              total        used        free      shared  buff/cache
available
Mem:          996604      555340      408496           0       32768
397420
Swap:              0           0           0
```

Interface Information

```
root@prx126-sfp-pon:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: eth0_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1516 qdisc prio state
UNKNOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
   inet6 [redacted]:144/64 scope link
      valid_lft forever preferred_lft forever
3: eth0_0_1_lct: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
UNKNOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
   inet 192.168.11.1/24 brd 192.168.11.255 scope global eth0_0_1_lct
      valid_lft forever preferred_lft forever
   inet6 [redacted]:17c2/64 scope link
      valid_lft forever preferred_lft forever
4: eth0_0_2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group
default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
5: eth0_0_3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group
default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
6: eth0_0_us: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group
default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
7: ins0: <BROADCAST,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UNKNOWN group default qlen 1000
   link/void 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
8: pon0: <BROADCAST,MULTICAST> mtu 1500 qdisc prio state DOWN group
default qlen 1000
   link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

```
9: ip0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default
qlen 1000
   link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
10: tcont-omci@pon0: <BROADCAST,MULTICAST,M-DOWN> mtu 1500 qdisc noop
state DOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
11: gem-omci@pon0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP,M-DOWN> mtu
2030 qdisc pfifo_fast state UNKNOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
12: iphost1_bp@ip0: <BROADCAST,MULTICAST,M-DOWN> mtu 1500 qdisc noop state
DOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
13: iphost1@iphost1_bp: <BROADCAST,MULTICAST,M-DOWN> mtu 1500 qdisc noop
state DOWN group default qlen 1000
   link/ether [redacted] brd ff:ff:ff:ff:ff:ff
```

Mounted Partitions

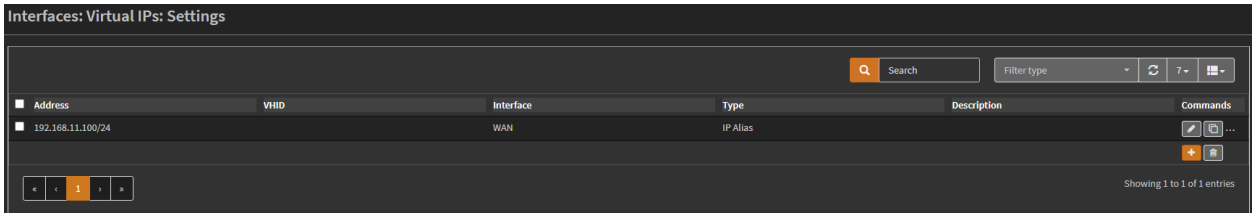
```
root@prx126-sfp-pon:/tmp# mount
/dev/root on /rom type squashfs (ro,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,noatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noatime,mode=01777)
ubi0_6 on /overlay type ubifs (rw,noatime)
overlayfs:/overlay on / type overlay
(rw,noatime,lowerdir=/,upperdir=/overlay/upper,workdir=/overlay/work)
ubi0:ptconf on /ptconf type ubifs (rw,sync,relatime)
ubi2:ptdata on /ptdata type ubifs (ro,relatime)
pstore on /sys/fs/pstore type pstore (rw,relatime)
tmpfs on /dev type tmpfs (rw,nosuid,relatime,mode=0755,size=512K)
devpts on /dev/pts type devpts
(rw,nosuid,noexec,relatime,mode=600,ptmxmode=000)
debugfs on /sys/kernel/debug type debugfs (rw,noatime)
```

Router specific information

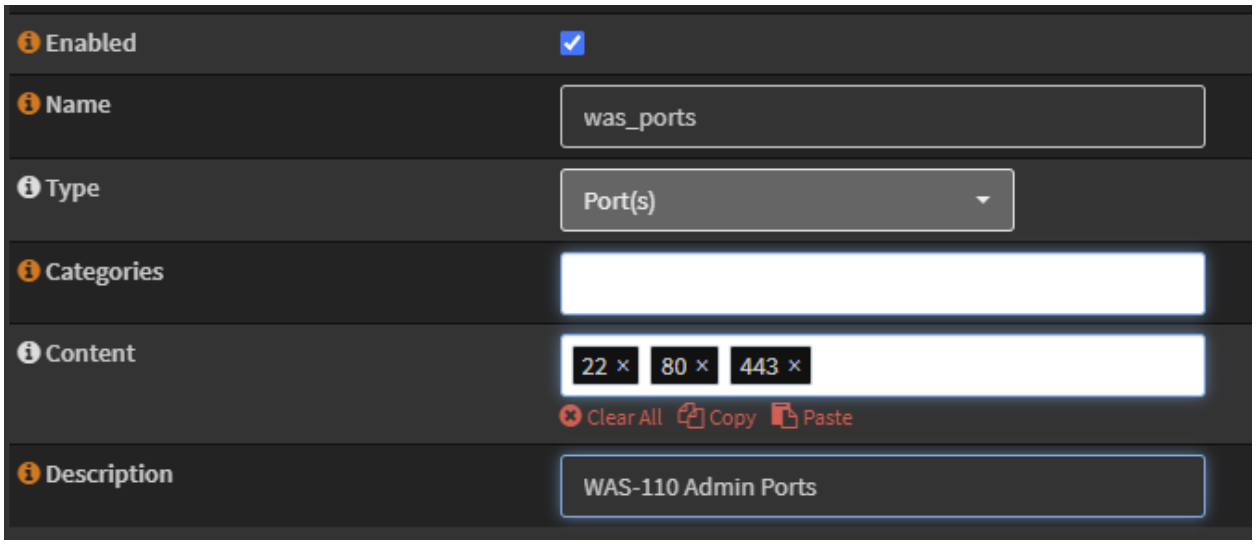
Accessing the stick from your LAN

OPN/pfSense

Under “Interfaces” create a new virtual IP as shown and apply it to the appropriate WAN interface (WAN for primary or single, WAN2 for secondary etc)

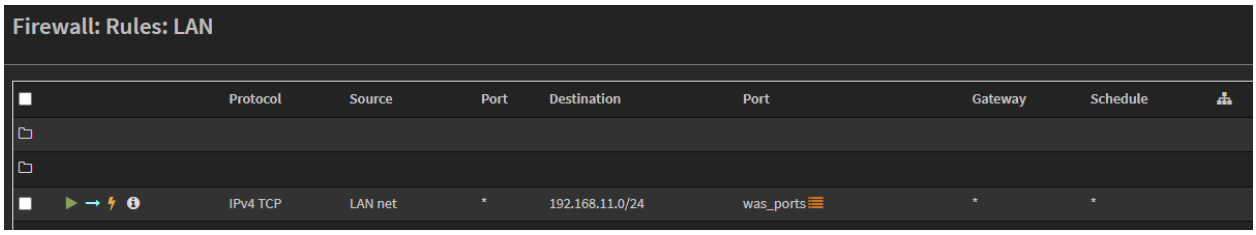


Create an alias for your WAS admin ports (22,80,443) under “Firewall”



Finally, create an Outbound NAT rule. The source should be the IP/network you want to perform administration from, it is not recommended for this to be “any”. The destination should be the default network of the WAS with the alias selected as the ports. On pfSense, your translation address will be 192.168.11.100 instead of “Interface address”

Finally confirm you have a firewall rule allowing your selected network into the LAN network. On OPNSense this is cover by the default allow, if you have removed this you will need to make a new one



Ubiquiti

To access the stick you need to run the following command inside of your Ubiquiti device, such as a UDM-Pro, to add the route. Assuming you are using the top SFP+ port (port 10 on UDM-Pro; you can confirm which network interface to use instead of `eth9` with `ifconfig` and finding the interface that has your active WAN IP):

```
ip route add 192.168.11.0/24 dev eth9
```

Then you can SSH or telnet from the UDM-Pro into the stick. You should also be able to access 192.168.11.1 from anywhere on your LAN but YMMV. The route shouldn't cause issues as long as your network isn't also 192.168.11.0/24 but just in case to remove the route later:

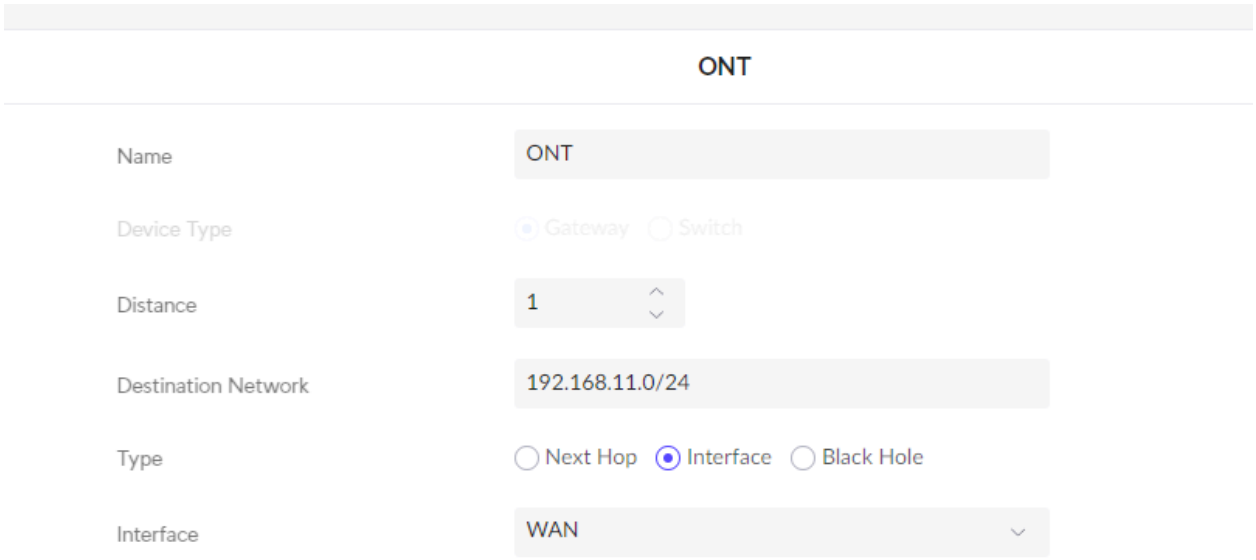
```
ip route del 192.168.11.0/24
```

By default UniFi OS doesn't include `telnet` but you can use netcat like this:

```
nc -v 192.168.11.1 23
```

The terminal will be a little messed up in places but it is fully functional

Others mention reports of just adding a static route:



Using AT&T static IPs

Ubiquiti

This setup will enable routing of your AT&T static IPs. The script will poll AT&T's DHCP server for updates to keep static IPs alive, allowing you to set your DHCP IP as "static" in the Internet section. A bonus of this specific setup is you should be able to use every IP in the block, including the network, gateway and broadcast IPs. The script will also automatically add the route to access the SFP config system at startup of your device. This has been tested on UniFi OS 3.0.20. The script assumes the stick is installed on the UDM-Pro's WAN SFP+ port which is labeled port 10 and is internally known as `eth9`. If you have installed it in the LAN port you should change all `eth9` references to `eth8`.

Credit goes to @1NightFury on the Discord, this UniFi forum post and this guide

Instructions

1. Install the UDM / UDMPro Boot script
2. Find your DHCP provided IP address
3. Replace `PUBLIC_DHCP_IP` in the script with your DHCP provided IP address
4. Set your WAN IPv4 Connection to Static IP and enter your DHCP provided IP address, netmask (can be calculated with output of `ip a`, e.g. 23.124.111.157/23 would mean netmask of 255.255.254.0) and gateway IP (easiest found by getting it from the first line of `traceroute 8.8.8.8`, it should end in .1)

5. Add your static IP block to Additional IP addresses
6. Place this script at `/data/on_boot.d/07-renew-public-att-dhcp.sh`
7. Place the logrotate config (below) at `/etc/logrotate.d/udhcpc` to ensure the log file doesn't fill up
8. Reboot your UDM
9. Confirm DHCP started up by running `cat /var/log/udhcpc.log`

Notes:

- You may need to add the following lines to the bottom of the script in order to route traffic to the WAN again, replacing ATT_DHCP_GATEWAY_IP with your Gateway IP found above:

```
- ip route add ATT_DHCP_GATEWAY_IP dev eth9
- ip route add default via ATT_DHCP_GATEWAY_IP dev eth9
```

DHCP refresh script

```
#!/bin/bash
#/data/on_boot.d/07-renew-public-att-dhcp.sh

# From the PON Madness guide created by the 8311 Discord. Latest updates
at
https://docs.google.com/document/d/1UIAgtxkImgFRwyaGDGtISD0JXnxWNvuuNDrnRa
c6wGc/edit

nohup /usr/bin/busybox-legacy/udhcpc --foreground --interface eth9
--script /usr/share/ubios-udapi-server/ubios-udhcpc-script -r
PUBLIC_DHCP_IP >/var/log/udhcpc.log 2>&1 &

# Add a route to be able to access the SFP+ stick via telnet/SSH
ip route add 192.168.11.0/24 dev eth9
```

Logrotate config

```
# /etc/logrotate.d/udhcpc
# Rotate the logs to keep them from filling up the system
```

```
/var/log/udhcpc.log {
	weekly
	rotate 1
	size 100K
	compress
	delaycompress
}
```

NetworkManager (Linux-as-a-router)

IPv4

You should set the `ipv4.method` to `auto`. If you have any static IPv4s, you can additionally add them to `ipv4.addresses`, but be sure not to reset `ipv4.method` back to `manual`.

If you have static addresses assigned to you, you must first request a DHCP address before you are able to use the static address block. Traffic will be blocked until you complete the DHCP request.

```
# nmcli conn edit attfiber

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'attfiber'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet
(ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4, ipv6, hostname, tc,
proxy
nmcli> set ipv4.method auto
Do you also want to clear 'ipv4.addresses'? [yes]: yes
nmcli> set ipv4.addresses 192.168.11.2/24, 104.555.555.555/29
Do you also want to set 'ipv4.method' to 'manual'? [yes]: no
nmcli> save
```

IPv6

There are a few peculiarities when setting up your DHCPv6 client. You must have the DUID method set to `DUID-EN` with enterprise ID 3561. If you want DHCPv6 leases to work immediately, you'll need to calculate the DUID your AT&T gateway uses with the [gen-duid.sh] script from `pfatt`.

The DHCPv6 server will accept requests for Identity Associations of the type `IA_NA` (non-temporary address) and `IA_PD` (prefix delegation) addresses. However, the `IA_NA` returned will be non-routed and only appears to be used to associate the Prefix Delegation with

your lease. If you want to be able to originate IPv6 connections from your router/firewall, you'll need to use one of the delegated prefixes (e.g., a /64 network from the /60 delegation) and assign it to the WAN side of your Linux box. It doesn't appear to matter which address is chosen.