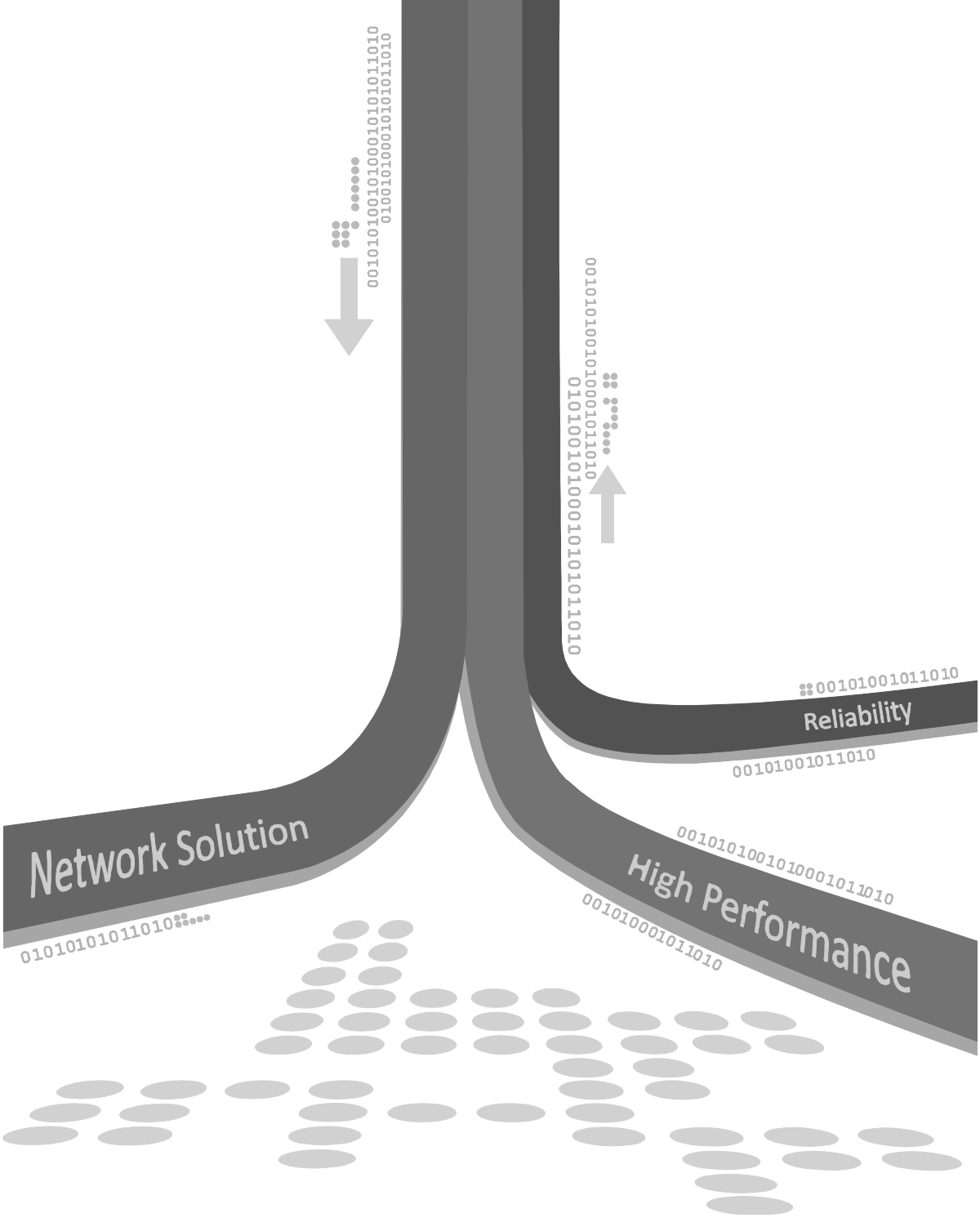


H640GW

GPON ONT with VoIP & Wi-Fi

Admin Manual

Issued by Technical Documentation Team
Korea

Reason for Update

Summary: Issue No.02

Details:

Chapter/Section	Reason for Update
3.2.2	NOTE regarding DNS configuration added
4.1.1, 4.1.2	NOTE regarding user account added
4.2	"Status Information" added
4.3.2	"LAN connection" added
4.3.3	"DHCP Client" added
4.3.4	"Wireless LAN" added
4.4	"Advance Settings" added
4.5	"System Management" added

Issue History

Issue Number	Date of Issue	Reason for Update
01	04/2013	Initial release
02	06/2013	Update for Web Management (NOS 2.25-1025)

Contents

Illustrations

1 Introduction

1.1 Audience

This manual is intended for the H640GW GPON ONT system operators and maintenance personnel for providers of Gigabit Passive Optical Network (GPON) and Ethernet services. This manual assumes that you are familiar with the following:

- Ethernet networking technology and standards
- Internet topologies and protocols
- GPON technology and standards
- Usage and functions of graphical user interfaces.

1.2 Document Convention

This guide uses the following conventions to convey instructions and information.

Information

This symbol indicates useful information when using configuration commands. The information notes contain helpful suggestions or references.

Warning

This symbol warns of a situation that could cause bodily injury or equipment breakdown. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by turning to this warning message.

2 Product Overview

DASAN Networks' H640GW optical network terminal is targeted for all subscribers requiring multiple FXS and high-speed data interfaces in a cost-effective indoor housing. Fully compliant with ITU-T G.984 standards, the H640GW supports data rates of 1.2Gbps upstream and 2.5Gbps downstream. With DASAN's leading-edge GPON technology, users can enjoy bandwidth-intensive multimedia services such as real-time video, audio and gaming much easier and faster than ever before.

The H640GW has one GPON uplink port, and provides two FXS voice / four Gigabit Ethernet (10/100/1000Base-T) interfaces and Wireless LAN service. The H640GW supports the full Triple Play of services including voice, video (IPTV), and high-speed Internet access service.

The H640GW contains both built-in wire-speed L2 switch and L3 routing gateway with port forwarding, NAT address translation, and PPPoE client support for high-speed Internet service.

Service Scenario for GPON with H640GW

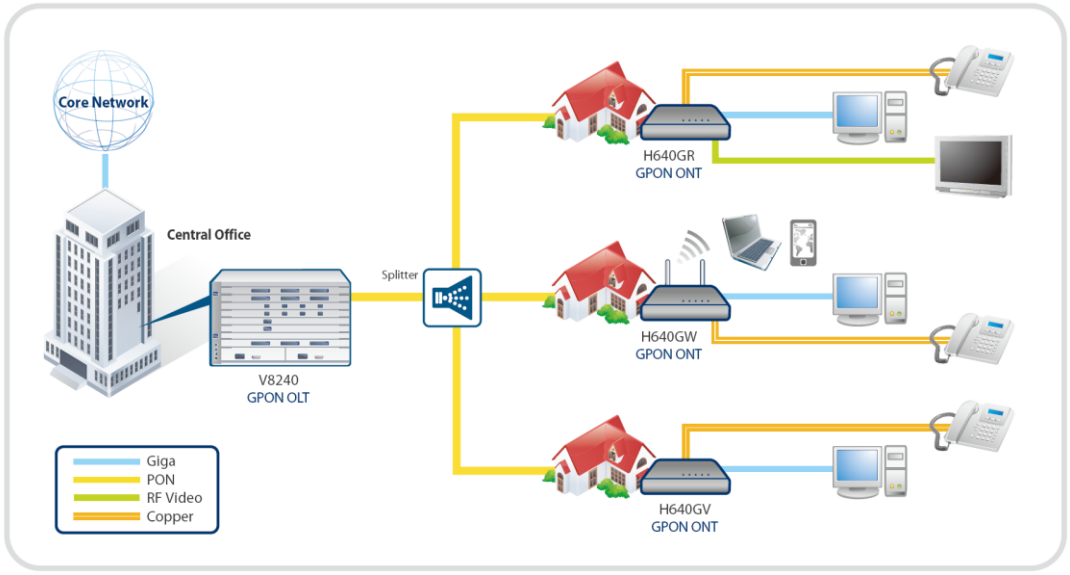


Fig. 2.1 Service Scenario for GPON with H640GW

A PON consists of an Optical Line Termination (OLT) located at the Central Office and a set of Multi Dwelling Units (MDUs) or Optical Network Terminals (ONTs) located at the customer's premises. Between them is the optical distribution network (ODN) comprised of fibers and passive optical splitters or couplers. A splitter is a device that divides an optical signal into two or more signals. The OLT connects the PON to the IP network that controls and manages the PON clients. An MDU (ONT) connects the user- specific network to the PON. The ONT can be utilized by a single subscriber or used as a multi-dwelling gateway for a local network.

3 Basic Configuration via OLT

Before the basic configuration for the connection to WAN, you should install the unit correctly first. To see how to install the unit, refer to the QIG (Quick Guide) for this unit.

Basically, to connect this unit to the WAN for VoIP and the Internet services, you should have the unit get the basic configuration via OLT. The following sections explain how to perform the configuration on the connected OLT.

i For the detail description of each command and related option in the following sections, refer to the User Manual (CLI) of OLT.

3.1 Upgrade of ONT

You may have to upgrade ONT first for the purpose of perfect support for the services before the basic ONT configuration.

The following command lines show an example for the ONT upgrade.

```
OLT# copy tftp onu down ❶
       To exit : press Ctrl+D
-------------------------------------
IP address or name of remote host (TFTP): 10.45.33.227
Download File Name : G_ONU_N_NewVersion.H640OO.x
Now 10.45.33.227 ONU Firmware download from via tftp.
Downloading file ....
Received 16058792 bytes

OLT(config-gpon-olt[2/2])# onu upgrade 2 G_ONU_N_NewVersion.H640OO.x ❷
...

OLT(config-gpon-olt[2/2])# show onu firmware version 2 ❸
                                          (D):Default-OS (R):Running-OS
-------------------------------------------------------------------------
  OLT | ONU |     Upgrade Status     |          OS1         |         OS2
-------------------------------------------------------------------------
  2/2 |  2  |    Commit Complete     | (D) NewVersion |  (R) OldVersion

OLT(config-gpon-olt[2/2])# onu reset 2 ❹
```

❶ Download ONT OS file to OLT

❷ Upgrade ONT with the downloaded OS

❸ Check out the upgrade result

❹ Reboot the ONT. The ONT will be restarted with "Default-OS (*NewVersion*)".

3.2 Basic Configuration via OLT

Basically, it is required that a series of configuration including traffic profile and IP host is predefined at the ONT in order to get access to the Internet and serve the VoIP and data service. This section describes how to have the ONT get the configuration, with a detail sample config on the basis of a sample scheme, for easier understanding and usage of config copy.

The following diagram shows a sample scheme for it.

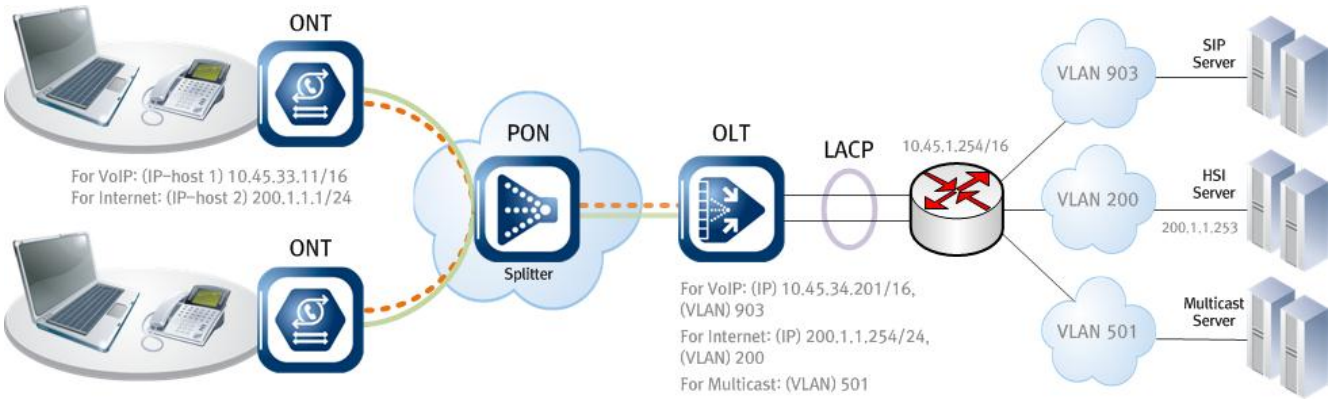


Fig. 3.1 PON Structure Sample Scheme for VoIP and Internet Connection of ONT

3.2.1 Pre-Settings for Traffic Profile (Step 1)

The following config command lines show a sample config for pre-settings of traffic-profile corresponding to the sample scheme above.

```
OLT(gpon)# show running-config
...
gpon
...
olt multicast-gem 4094 ❶
olt interwork igmp-snooping enable
!
...
dba-profile BE create ❷
  mode sr
  sla fixed 128
  sla maximum 1031616
  apply
!
dba-profile VOIP create ❷
  mode sr
  sla fixed 128
  sla maximum 4096
  apply
!
...
multicast-profile V501 create ❸
  igmp tag-control add vid 501 cos 0
  igmp access-list vid 501 dst-ip start 224.0.0.1 end 239.255.255.255 gem 4094
```

```
  apply
!
...
 extended-vlan-tagging-operation V200 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 200 cos 0 tpid 0x8100
  apply
 !
 extended-vlan-tagging-operation V903 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 903 cos 0 tpid 0x8100
  apply
!
extended-vlan-tagging-operation V501 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 501 cos 0 tpid 0x8100
  apply
 !
...
voip-profile SIP create ❺
  codec-nego 1 codec pcma packet-period 10 silence-suppression 1
  codec-nego 2 codec pcmu packet-period 10 silence-suppression 1
  codec-nego 3 codec g729 packet-period 10 silence-suppression 1
  codec-nego 4 codec g723 packet-period 10 silence-suppression 1
  protocol sip
   proxy-server 10.45.2.1
   outbound-proxy-server 10.45.2.2
   register-server 10.45.2.3
   host-part-server 10.45.2.4
   dns primary 168.126.63.1
  apply
!
...
```

❶ Add a specific GEM port ID (`4094`) to the multicast stream.

❷ Create DBA profiles (`BE` - for Internet service, `VOIP` - for VoIP service). And then configure the corresponding settings.

❸ Create a multicast profile (`V501`). And then configure the corresponding settings.

❹ Create extended VLAN tagging operation profiles (`V200` - for Internet service, `V903` - for VoIP service, `V501` - for multicast service). And then configure the corresponding settings.

❺ Create a VoIP profile (`SIP`). And then configure the corresponding settings.

3.2.2 Traffic Profile Configuration (Step 2)

The following command lines show a sample config of traffic profile corresponding to the sample scheme. You can find out which configurations are required for ONT's VoIP and data service through each annotation.

```
OLT(gpon)# show running-config traffic-profile TRAFFIC

traffic-profile TRAFFIC create ❶

 mgmt-mode uni eth 1 non-omci link virtual-eth 1 ❷
 mgmt-mode uni eth 2 omci
 mgmt-mode uni eth 3 omci
 mgmt-mode uni eth 4 omci

 tcont 1
  gemport 1/1-1/4
  dba-profile BE ❸
 tcont 2
  gemport 2/1-2/4
  dba-profile BE ❸
 tcont 3
  gemport 3/1
  dba-profile VOIP ❸
 mapper 1
  gemport count 4
 mapper 2
  gemport count 4
 mapper 3
  gemport count 1

 bridge 1
  ani mapper 1
  uni eth 1
   extended-vlan-tagging-operation V200 ❹

 bridge 2
  ani mapper 2
  uni eth 2
   multicast-profile V501 ❺
   extended-vlan-tagging-operation V501 ❹
  uni eth 3
   multicast-profile V501 ❺
   extended-vlan-tagging-operation V501 ❹
  uni eth 4
   multicast-profile V501 ❺
   extended-vlan-tagging-operation V501 ❹

 bridge 3
  ani mapper 3
  link ip-host-config 1

 ip-host-config 1 ❻
  ip address static
  dns primary 168.126.63.1
  link voip-service 1
  extended-vlan-tagging-operation V903

 ip-host-config 2 ❼
  ip address static
  extended-vlan-tagging-operation V200
```

```
  voip-service 1 ❽
   manage-method omci
   voip-profile SIP
   uni pots 1
   uni pots 2
  apply
!
```

❶ Create a traffic profile (`TRAFFIC`).

❷ If you want to set "Bridge", then you should use `omci`.
Otherwise, if you want to set "NAT" or "PPPoE", then you should use `non-omci`.
Basically, `non-omci` configures an interface as "NAT". For the PPPoE, PPPoE enabling on web interface is required additionally. For detail information of PPPoE enabling, see 4.3.1 PPPoE Configuration on "Internet Connection" Menu.

❸ Associate the created DBA profiles (`BE` - for Internet & multicast service, `VOIP` - for VoIP service) to T-CONT.

❹ Associate the created extended VLAN tagging operation profile to each Ethernet port (`extended-vlan-tagging-operation V200` - for Internet service (`eth 1` in this config), `extended-vlan-tagging-operation V501` - for multicast service (`eth 2` to `eth 4` in this config)).

❺ Associate the created multicast profile (`V501`) to the Ethernet ports for multicast service (`eth 2` to `eth 4` in this config).

❻ Configure `ip-host-config 1`.
The `ip-host-config 1` is a host only for VoIP.
- Configure IP address assignment (`static` in this config).
- Associate a VoIP service (`voip-service 1`) to this configuration (`ip-host-config 1`).
- Associate the created extended VLAN tagging operation profile (`extended-vlan-tagging-operation V903`) to this configuration (`ip-host-config 1`).

❼ Configure `ip-host-config 2`.
The `ip-host-config 2` is a host only for `non-omci`-configured interfaces.
- Configure IP address assignment (`static` in this config).
- Associate the created extended VLAN tagging operation profile (`extended-vlan-tagging-operation V200`) to this configuration (`ip-host-config 2`).

i In case of `ip address static`, it is required to configure DNS. Otherwise, it is set to the DASAN-specified value, by default, which may cause to limit any service.

❽ Create a VoIP service (`voip-service 1`) to be associated to IP host configuration for VoIP (`ip-host-config 1`). And then configure the corresponding settings. Here, associate the created VoIP profile (`SIP`).

3.2.3 ONU Profile & IP Host Configuration (Step 3)

The following command lines show a sample config for OLT port corresponding to the sample scheme above.

```
OLT(gpon)# show running-config
```

```
...
onu-profile ONU create ❶
  traffic-profile TRAFFIC
  apply
!
...

OLT(config-gpon-olt[2/2])# show running-config gpon-olt 2/2
gpon-olt 2/2
  olt auto-to-manual enable
  olt anti-spoofing enable expire-timeout 60
  discover-serial-number start 10
  onu add 2 DSNW4bd68b38 auto-learning ❷
  onu-profile 2 ONU ❸
  onu static-ip 2 ip-host 1 10.45.33.11/16 gw 10.45.1.254 ❹
  onu static-ip 2 ip-host 2 200.1.1.1/24 gw 200.1.1.254 ❹
  onu voip-sip 2 phone-number pots 1 07070177670
  onu voip-sip 2 auth pots 1 07070177670 39588102947
```

❶ Create an ONU profile (`ONU`). And then configure the corresponding settings. Here, associate the created traffic profile (`TRAFFIC`) to this profile (`ONU`).

❷ Register an ONT (`DSNW4bd68b38`) to the OLT with specifying its ID (`2`).

❸ Apply the created ONU profile (`ONU`) to the specified ONT (OLT port: `2/2`, ONU ID: `2`).

❹ Assign the planned static IP addresses to the configured IP hosts (`ip-host 1` for POTS, and `ip-host 2` for LAN1 port on sample config in this guide). Here, `ip-host 1` uses network 10.45.x.x, and `ip-host 2` uses 200.1.1.x.

i To assign static IP address to the IP hosts, `ip address static` should be set in `ip-host-config` of traffic profile first.

i The `ip-host 1` is a host only for VoIP, and the `ip-host 2` is a host only for `non-omci`-configured interfaces.

i If you want to have the VoIP host assigned the same IP as NAT host, you should perform the following: All of the POTS interfaces have to be set to `non-omci` (`mgmt-mode uni pots 1 non-omci` and `mgmt-mode uni pots 2 non-omci`). This tells an IP host binding. The `non-omci`-configured interfaces are all affected by `ip-host 2`.

You can check whether the IP hosts are assigned IP addresses normally and VoIP service is registered normally with the following commands.

```
OLT(config-gpon-olt[2/2])# show onu ip-host 2
-----------------------------------------------------------------
 OLT : 2/2, ONU : 2, Host : 1(0x0001)
-----------------------------------------------------------------
 IP Option           : Static ❶
 MAC Address         : 00:d0:cb:d6:8b:38
 Config IP           : 10.45.33.11 ❶
 Config Mask         : 255.255.0.0
 Config Gateway      : 10.45.1.254 ❶
```

```
 Config Primary DNS    : 168.126.63.1
 Config Secondary DNS  : 0.0.0.0
 Host name             :
----------------------------------------------------------------
 OLT : 2/2, ONU : 2, Host : 2(0x0002)
----------------------------------------------------------------
 IP Option             : Static ❶
 MAC Address           : 00:d0:cb:d6:8b:38
 Config IP             : 200.1.1.1 ❶
 Config Mask           : 255.255.255.0
 Config Gateway        : 200.1.1.254 ❶
 Config Primary DNS    : 0.0.0.0
 Config Secondary DNS  : 0.0.0.0
 Host name             :

OLT(config-gpon-olt[2/2])# show onu voip line 2
-------------------------------------------------------------------------
OLT : 2/2, ONU : 2, POTS : 1
-------------------------------------------------------------------------
Line Status                   : Registered ❷
Used Codec                    : Auto select
Session Type                  : Idle
1st Protocol Period / Dest Addr :  20 / 0.0.0.0
2nd Protocol Period / Dest Addr :  20 / 0.0.0.0

-------------------------------------------------------------------------
OLT : 2/2, ONU : 2, POTS : 2
-------------------------------------------------------------------------
Line Status                   : None/initial
Used Codec                    : Auto select
Session Type                  : Idle
1st Protocol Period / Dest Addr :  20 / 0.0.0.0
2nd Protocol Period / Dest Addr :  20 / 0.0.0.0
```

❶ Check whether IP host configuration is applied normally. (`Host 1` for VoIP, `Host 2` for Internet service)
Ping to the gateway (200.1.1.254) for checking connection with OLT by using PC connected to the ONT.
Ping to the HSI server (200.1.1.253) for checking Internet access by using PC connected to the ONT.

❷ Check whether the VoIP service is registered normally.

4 Web Management

The H640GW provides web-based management GUI interface for the user and administrator's easy configuration and maintenance. This chapter explains how to configure the ONT via the GUI interface.

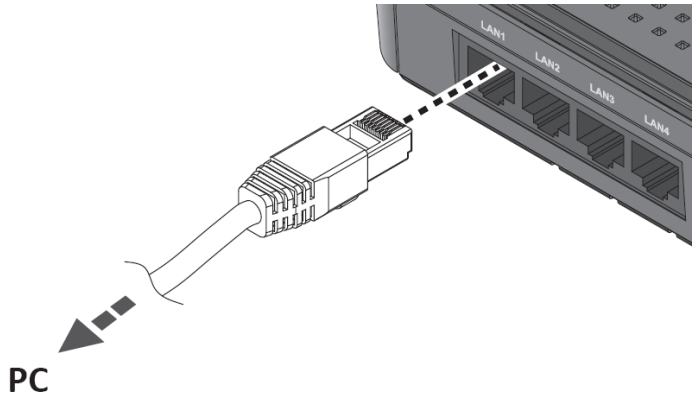
4.1 Initial Access

The H640GW supports two ways for you to get initial web-access; through direct PC connection to LAN port, or via remote access. For the details of how to get initial access, see the following sections.

4.1.1 Initial Access via LAN Port Connection

You can access the ONT's GUI interface by using the LAN port local connection. This method is useful when you do not know the IP address of ONT.

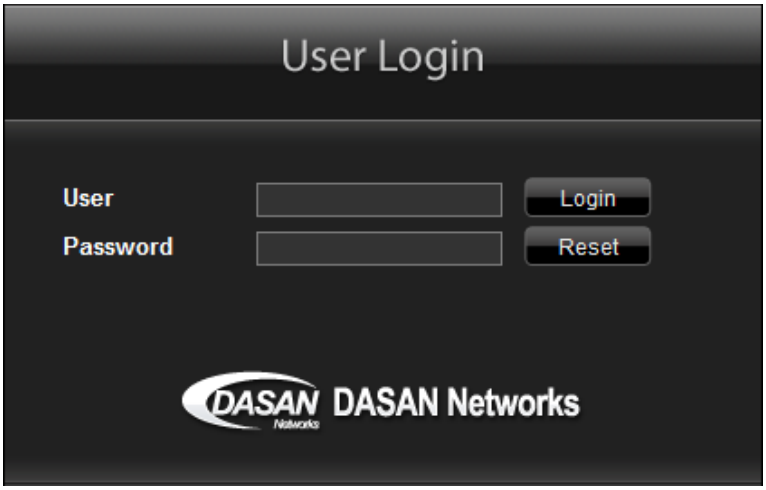
1. Connect your PC to the LAN port of the unit using an Ethernet cable.



2. Configure IP address of your PC to one of 192.168.1.1~254 (except 192.168.1.100).

i In case that the connected LAN port is configured as "NAT" mode (`mgmt-mode non-omci` in traffic-profile on OLT command line) and the PC is configured to be assigned IP by DHCP, this step can be omitted.

3. Open a web browser, and enter "http://192.168.1.100:8080" in a URL field, and then press Enter.



4. Type "admin/vertex25" in **User**/**Password** field, and log into the system by clicking **Login**. Initial page is displayed.

Basically, the ONT provides 2 types of accounts; admin and user. The admin is assigned the authority over all of the possible configurations, otherwise, the user account is limited on several admin-dedicated configurations. The account name and password for admin and user is "admin/vertex25" and "user/user" respectively.

4.1.2 Initial Access via Network Connection

You can access the ONT's GUI interface remotely in the same network.

You should know the ONT's IP address for the remote web access.
To know the address means that the ONT has been assigned a static IP address through `onu static-ip ip-host` command via OLT. Therefore, you can find out the address by `show onu ip-host` on OLT command line. For more information, see 3.2.3 ONU Profile & IP Host Configuration (Step 3).

1. Connect your PC to the network.
2. Open a web browser, and enter "http:///*IP_ADDRESS*:8080" in a URL field, and then press Enter.
3. Type "admin/vertex25" in **User**/**Password** field, and log into the system by clicking **Login**. Initial page is displayed.

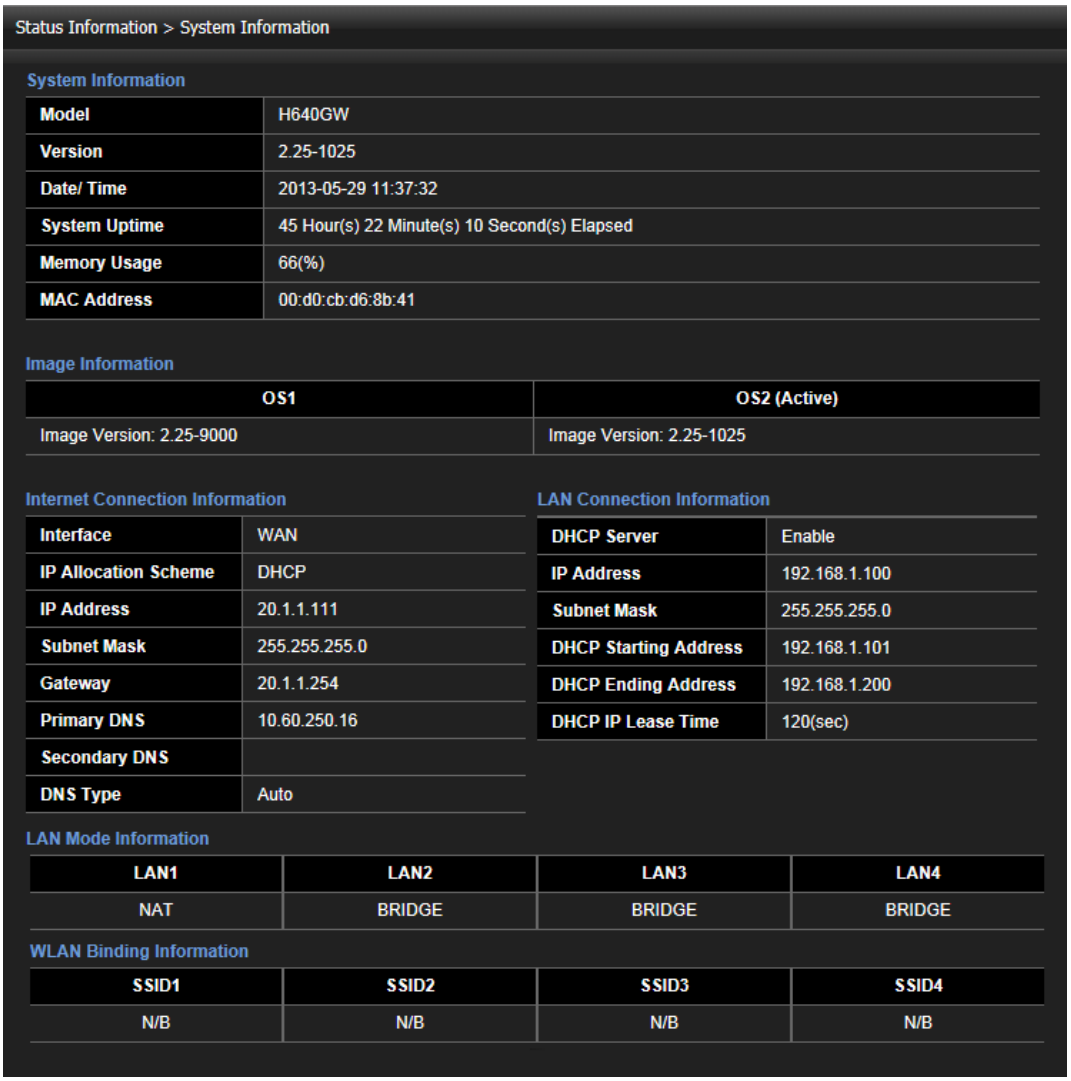
Basically, the ONT provides 2 types of accounts; admin and user. The admin is assigned the authority over all of the possible configurations, otherwise, the user account is limited on several admin-dedicated configurations. The account name and password for admin and user is "admin/vertex25" and "user/user" respectively.

4.2 Status Information

The **Status Information** provides the current system information, DHCP lease time of clients, and the scanned APs around the ONT. The submenus in this menu are only for your reference, not providing configurations.

4.2.1 System Information

You can check the system information on **System Information** in **Status Information**.



- **System Information**

This section shows the system basic information of ONT. The **Date/Time** is a current date and time.

- **Image Information**

The ONT supports dual OS. One of the two OS areas is operating (active), and the other is in a state of standby. The dual OS system means that you can upgrade OS through one OS area without aborting the service to the LAN and Wi-Fi.

After the ONT upgrade, you can operate a new version of firmware by changing default OS (`onu firmware commit` command on OLT) and restarting the ONT.

- **Internet Connection Information**

This section shows the IP address assigned to the ONT. For the details for how to configure IP address of ONT, see `ip-host-config 2` configuration part on 3.2.2 Traffic Profile Configuration (Step 2), and onu IP address configuration part on 3.2.3 ONU Profile & IP Host Configuration (Step 3).

- **LAN Connection Information**

The ONT supports NAT function and DHCP assignment. This section shows the private IP address assignment related to this function. For the details on configuration of LAN connection, see 4.3.2 LAN connection.

- **LAN Mode Information**

You can see the mode configuration (NAT or Bridge) by each Ethernet LAN port. For the details on configuration of NAT or Bridge mode, see `mgmt-mode` part on 3.2.2 Traffic Profile Configuration (Step 2).

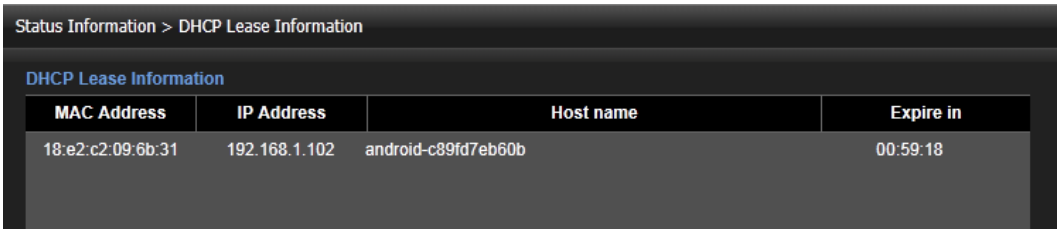
- **WLAN Binding Information**

This section shows the status of SSID binding for wireless traffic bridging. The "N/B" means NAT Binding, and B/B, Bridge Binding. For the details on configuration of SSID binding, see 4.3.4.3 SSID Bridge Bind.

The web management does not provide the information and configuration on VoIP. It is allowed only on the connected OLT.

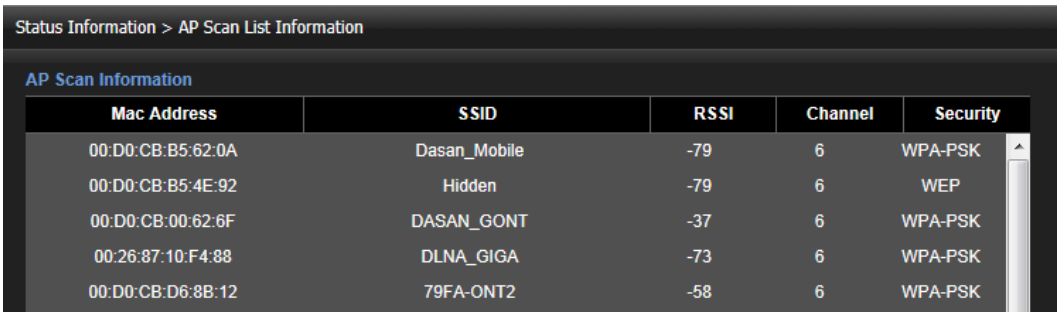
4.2.2 DHCP Lease Information

Through this menu, you can check the MAC address (**MAC Address**), assigned IP address (**IP Address**) and DHCP lease remaining time (**Expire in**) of ONT's clients (**Host Name**). The following is a sample screen of **DHCP Lease Information**.



4.2.3 AP Scan List Information

This screen shows the AP's list scanned around the ONT. The following is a sample screen of **AP Scan List Information**.


Status Information > AP Scan List Information
AP Scan Information
Mac Address
SSID
RSSI
Channel
Security
00:D0:CB:B5:62:0A
Dasan_Mobile
-79
6
WPA-PSK
00:D0:CB:B5:4E:92
Hidden
-79
6
WEP
00:D0:CB:00:62:6F
DASAN_GONT
-37
6
WPA-PSK
00:26:87:10:F4:88
DLNA_GIGA
-73
6
WPA-PSK
00:D0:CB:D6:8B:12
79FA-ONT2
-58
6
WPA-PSK

4.3 Basic Settings

The **Basic Settings** provide the configuration for WAN (**Internet Connection**) and LAN.

Basically, the admin can only access to **Internet Connection** menu. However, if the admin makes a user have authority to configure WAN, a user can access to it as well. For the details for granting WAN configuration authority to a user, see "User WAN Configure" part on 4.5.2 Admin Access Management.

The **DHCP** or **Static IP** configuration on **Internet Connection** is for assignment of ONT IP address from WAN in order to operate NAT. Basically, the ONT's IP address is only assigned through the connected OLT, therefore, the assignment is not allowed on the ONT's web interface. For the details for how to configure IP address of ONT, see `ip-host-config 2` configuration part on 3.2.2 Traffic Profile Configuration (Step 2), and onu IP address configuration part on 3.2.3 ONU Profile & IP Host Configuration (Step 3).

4.3.1 PPPoE Configuration on "Internet Connection" Menu

The Point-to-Point Protocol (PPP) is a data link protocol used in establishing a direct connection between two networking nodes, and it provides connection authentication, transmission encryption, and compression. And the Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating those PPP frames inside Ethernet frames. The H640GW provides PPPoE configuration through **Basic Settings** > **Internet Connection** menu. The PPPoE can be configured only through web management.

The PPPoE configuration is only applied to `non-omci`-configured interfaces. For information of `non-omci` configuration, see ❷ in 3.2.2 Traffic Profile Configuration (Step 2). The PPPoE-configured ONT requests authentication and IP assignment to a BRAS server.

1. Select **PPPoE** in **Mode** drop-down.
2. Select **Enable** radio button in **Enable**.
3. Select an authentication type in **Authentication**.

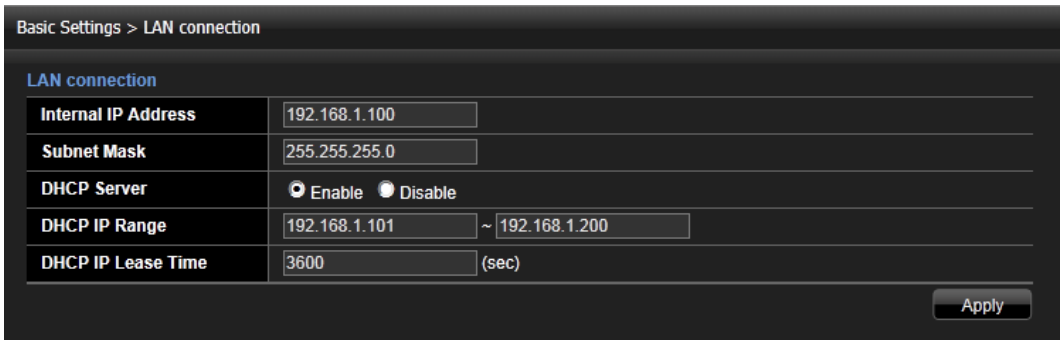
The Password Authentication Protocol (PAP) is an authentication protocol that uses a password. And the Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. That entity may be, for example, an Internet service provider. Generally, the CHAP provides better security as compared to PAP.

4. Enter a user account and password in **User** and **Password** respectively.

5. Click **Apply**.

4.3.2 LAN connection

In this menu, you can configure the settings regarding LAN connection toward ONT's clients. These settings apply only the terminal or another LAN connected to Ethernet port on NAT mode, and provide the configuration to assign the private IP addresses to terminals.



- **Internal IP Address**

Specify an ONT's internal private IP address. This is a gateway of ONT clients, and the IP address for initial access via LAN port connection. The factory default is "192.168.1.100". For the details of initial access via LAN, see 4.1.1 Initial Access via LAN Port Connection.

- **Subnet Mask**

Specify a subnet mask for IP address range of ONT's clients.

- **DHCP Server**

Configure the ONT as a DHCP server (**Enable**). If you disable the DHCP server, the ONT's clients cannot be assigned IP addresses. The settings below are valid only when **DHCP Server Enable** is selected.

- **DHCP IP Range**

Specify a DHCP IP address range for assignment to ONT's clients.

- **DHCP IP Lease Time**

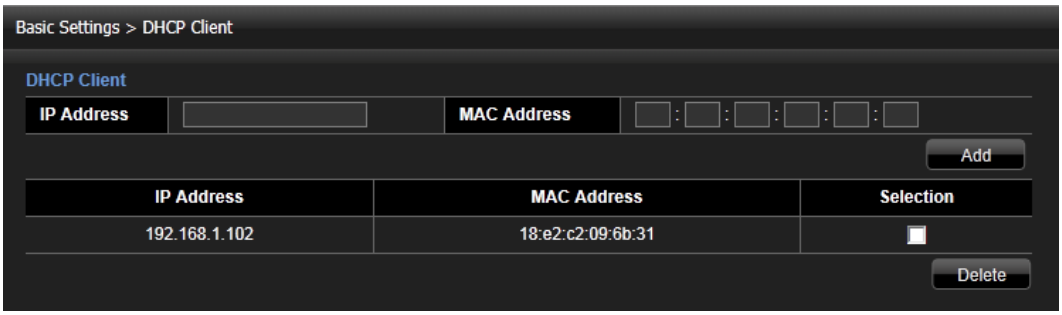
Specify a DHCP IP address lease time, which is applied to the DHCP-configured terminal or IP router connected to NAT of ONT.

i You should click **Apply** in order to reflect the configuration.

4.3.3 DHCP Client

You can configure a DHCP Fixed Address in this screen. A DHCP Fixed Address makes a particular IP address available for use exclusively by a single client (either to be wired or wireless-connected) (identified by MAC address). The client with this MAC address will always receive the designated IP address when connected to the ONT, and the designated IP address will never be allocated to any other MAC address.

i This configuration is applied only to the clients assigned IP address by NAT of ONT.



The following is the procedure of configuring a DHCP Fixed Address.

1. Enter an IP address in **IP Address**. You should specify an IP address within **DHCP IP Range** in **Basic Settings** > **LAN connection**.
2. Specify a MAC address of client in **MAC address**.
3. Click **Add**.

i A wrong type of IP or MAC address cannot be added.

To delete a configured DHCP fixed address, check **Selection** checkbox and click **Delete**.

4.3.4 Wireless LAN

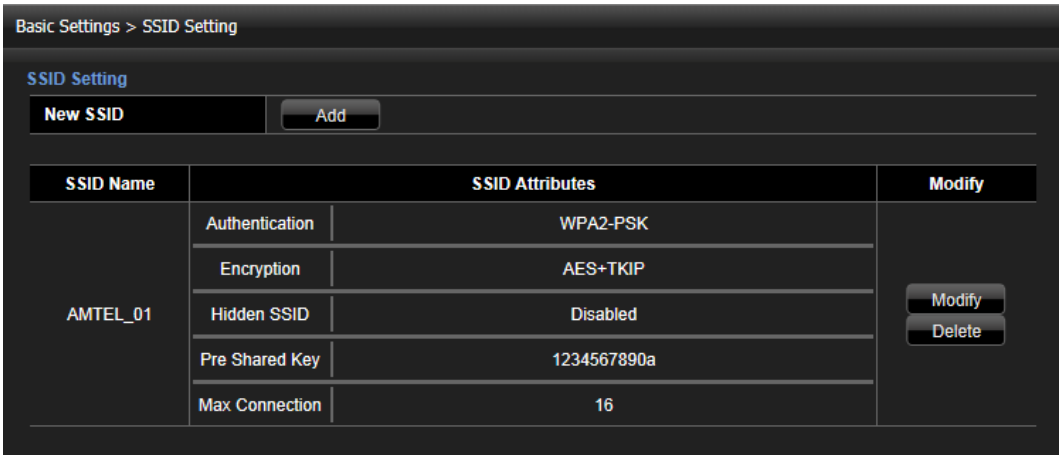
In this menu, you can configure the SSID-related settings.

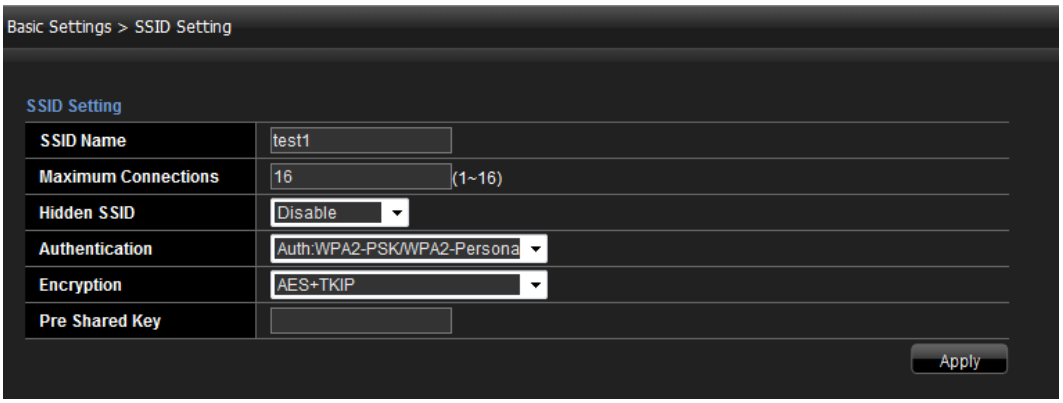
i The OLT cannot manage WLAN interface by using OMCI, because it has no communication interface for WLAN.

This menu consists of the following three submenus.

4.3.4.1 SSID Setting

You can create and manage SSIDs for wireless client access through this menu.





This following is a procedure of creating a new SSID.

1. Click **Add** in **New SSID**. A popup is displayed for creating a new SSID.
2. Enter an SSID name in **SSID Name**.
3. Specify a maximum number of connections. (1 to 16) in **Maximum Connections**.
4. Specify whether the SSID to be hidden (**Enable**) or not (**Disable**) in **Hidden SSID**. If an SSID is configured as hidden, it is not searched through scanning of wireless client.
5. Specify an authentication type in **Authentication**. The selections are as follows: **None**, **WPA-802.1x/WPA-Professional**, **WPA-PSK/WPA-Personal**, **WPA2-802.1x/WPA2-Professional**, **WPA2-PSK/WPA2-Personal**.
6. The **Encryption** is listed up depending on the selected authentication type. In case of authentication **None**, **None/WEP** are listed up as an encryption, and in case of authentication **WPA**, **AES/TKIP/AES+TKIP** listed up. Specify an encryption.
7. The additional settings are displayed below depending on the selected authentication or encryption type.
   • In case of authentication **None** and encryption **WEP**, specify a WEP key. Select a key type (**String** or **Hexadecimal**) in **WEP ASCII**, and choose a key type (**WEP64** or **WEP128**) again in **Key Type**. And then enter a WEP key in **Wep Key**. You can register up to 4 keys, one of which you can select to be applied.
   • In case of authentication **WPA-802.1x** or **WPA2-802.1x**, configure **Radius Server**, **Password**, and **Port**.
   • In case of authentication **WPA-PSK** or **WPA2-PSK**, configure **Pre Shared Key**.
8. Click **Apply**.

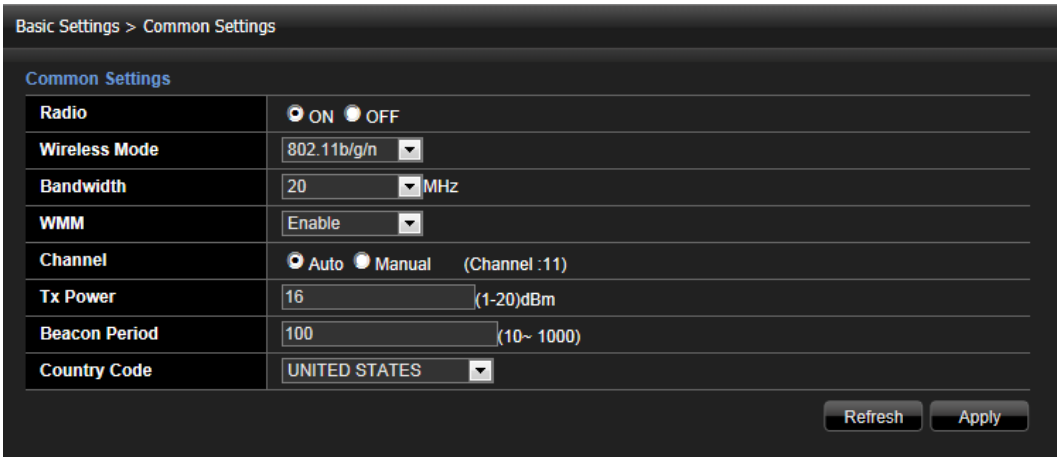
i You can create up to 4 SSIDs.

To modify an SSID configuration, click **Modify**, and change the settings. Click **Apply** to reflect changes.

To delete an SSID, click **Delete**.

4.3.4.2 Common Settings

In this menu, you can configure the common settings for wireless connection.



- **Radio**

Enable (**ON**) or disable (**OFF**) WLAN.

- **Wireless Mode**

Select a wireless mode.

i The IEEE 802.11 is a set of physical layer standards for implementing wireless local area network (WLAN) computer communication.

- **Bandwidth**

Specify a bandwidth.

- **WMM**

Enable or disable WMM.

- **Channel**

Specify a channel. In case you select **Auto**, the channel will be specified automatically. In case of **Manual**, you specify a channel in the expanded list. The channel number on the right side shows the current specified channel in case that the **Auto** is selected.

- **Tx Power**

Enter a TX power.

- **Beacon Period**

Enter a beacon period.

- **Country Code**

Select a country code.

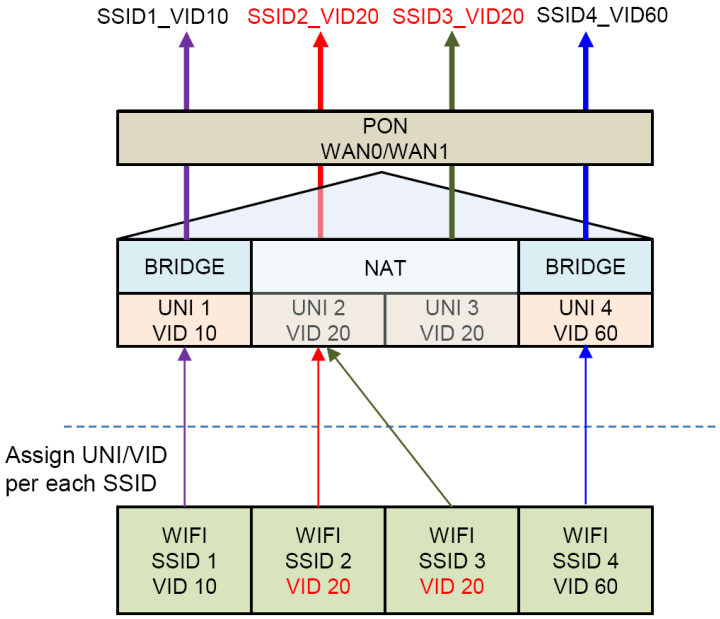
i If you want to restore the settings to the currently operating values during specification or selection, click **Refresh**.

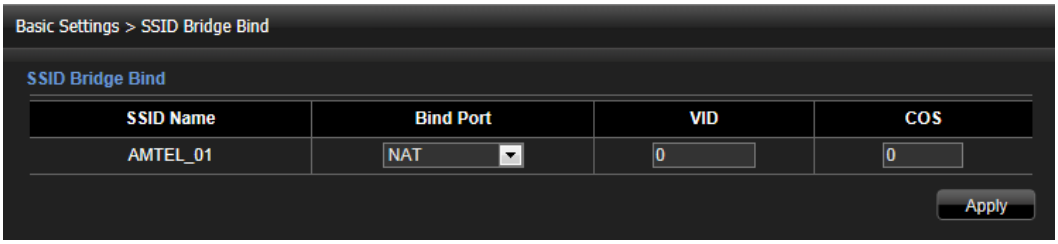
You should click **Apply** to reflect the configuration.

4.3.4.3 SSID Bridge Bind

i The **SSID Bridge Bind** menu can be accessed only by administrator ("admin" account).

Basically, the traffic of each WLAN client is transmitted with being bound to NAT or Bridge port. The ONT supports the admin configuration of the SSID binding to either NAT or Bridge port. However, the administrator needs to specify VLAN ID to each SSID as well, and this VLAN ID should be same as the one of a target UNI. The following is a sample diagram showing the SSID bridge binding. In the diagram, "SSID 1" is bound to "Bridge port UNI 1", and the VLAN is specified to "VID 10" because the "UNI 1" belongs to "VID 10".





The following is a procedure of SSID bridge binding.

1. Specify a bind target port in **Bind Port**. To bind to NAT port, select NAT. To bind to Bridge port, select a bridge port (one of LAN1 to LAN4). You can check out the mode of port at **Status Information** > **System Information**.
2. Enter a VID in **VID**. It should be same as the VID of a target UNI.
3. Enter a CoS in **COS**.
4. Click **Apply**.

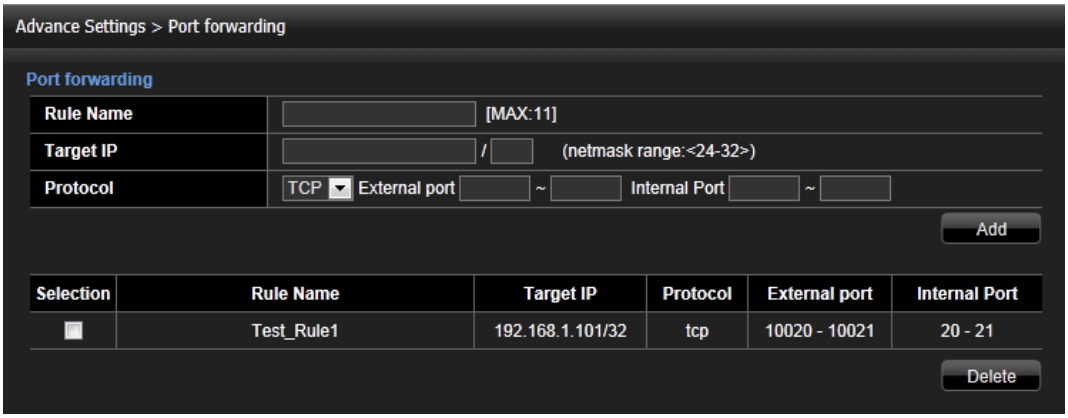
4.4 Advance Settings

The **Advance Settings** provide the configuration for port forwarding, DMZ and system service rule settings.

The settings in this menu are based on the NAT mode.

4.4.1 Port forwarding

The ONT supports the port forwarding that the external packets incoming through the specific port (service) is forwarded to the specific port (service) of the specific IP address.



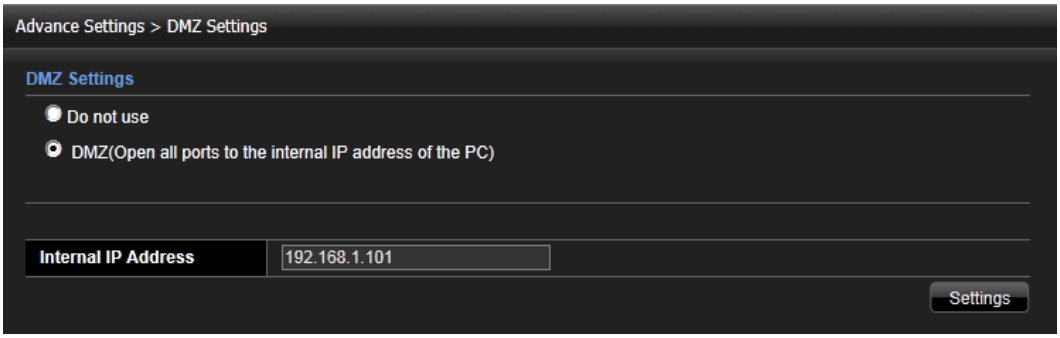
The following is a procedure of port forwarding configuration.

1. Enter a port forwarding rule name in **Rule Name**.
2. Enter a destination IP address to which the external packet is forwarded, in **Target IP**. And enter a netmask. If you create the rule by a single host, enter "32", otherwise, if by a range of hosts, enter a value of "24 to 30". (The configuration by netmask "24 to 30" is not currently supported.)
3. Select a protocol in dropdown of **Protocol**.
   If you need both of them with the same configuration, select **All**. In this case, two rules are created with suffixes of "_tcp" and "_udp".
4. Specify the range of port (service) to receive the external packets in **External Port**.
5. Specify the range of target port (service) on the client to send the packets to in **Internal Port**.
6. Click **Add**.

To delete a created rule, check **Selection** checkbox and click **Delete**.

4.4.2 DMZ Settings

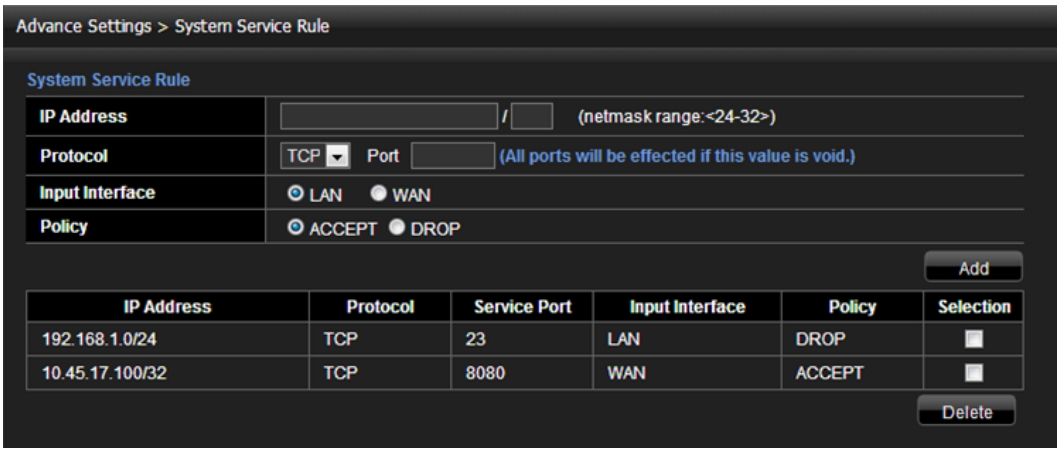
The ONT supports the DMZ feature to make all of the ports (services) on a client (PC) open to WAN, so that all of the incoming packets from WAN can be forwarded to the client.



To configure the DMZ setting, select **DMZ**. And then enter an IP address of internal target PC in **Internal IP Address**. Click **Settings**. The target PC will receive and handle all the packets from WAN.

4.4.3 System Service Rule

The ONT supports the filtering feature to permit or drop the packets from WAN or LAN based on specified service rules.



The following is a procedure of system service rule creation.

1. Enter a source IP address which transmits the packets, in **IP Address**. And enter a netmask. If you create the rule by a single host, enter "32", otherwise, if by a range of hosts, enter a value of "24 to 30".
2. Select a protocol in dropdown of **Protocol**. The possible selections are **TCP**, **UDP**, and **ICMP**. If you want to apply all of the protocols to the rule, select **Any**.
3. Enter a port (service) number (1 to 65535) in **Port**. To configure any of services applied, leave it blank.
4. Select **LAN** or **WAN** as a packet source in **Input Interface**.
5. Select **ACCEPT** or **DROP** as a policy in **Policy**.
6. Click **Add**.

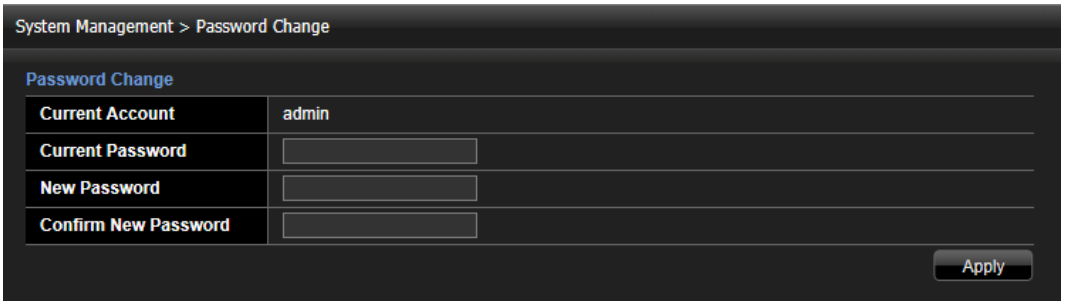
To delete a created rule, check **Selection** checkbox and click **Delete**.

4.5 System Management

The **System Management** provides the several configurations for system management.

4.5.1 Password Change

You can change the password of account currently logged in.



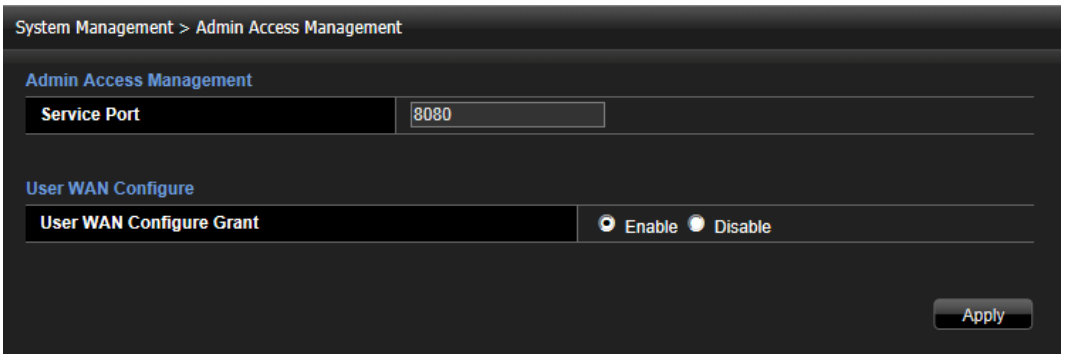
The following is a procedure of changing password.

1. Enter a current password in **Current Password**. You can check the current account at the top of table.
2. Enter a new password in **New Password**.
3. Enter the new password again in **Confirm New Password**.
4. Click **Apply**.

4.5.2 Admin Access Management

You can configure the admin access related settings in this menu.

This menu can be accessed only by administrator ("admin" account).



- **Admin Access Management**

You can change the service port for web access to this ONT. The default is "8080".

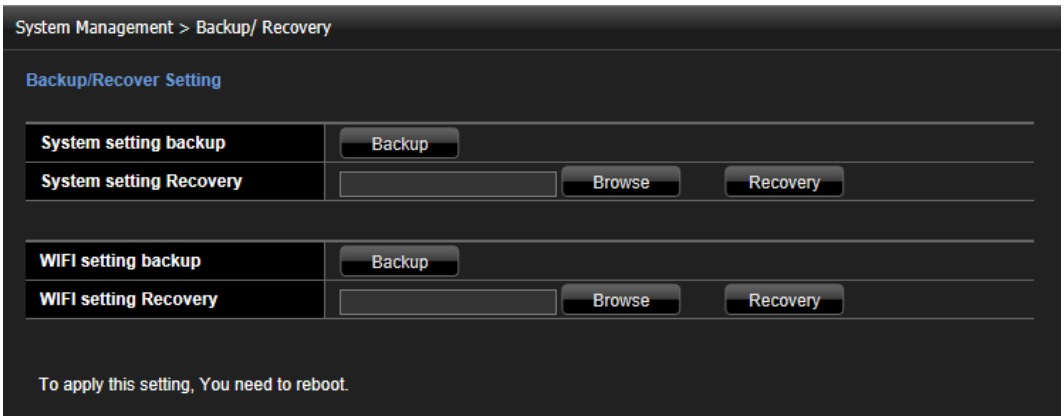
- **User WAN Configure**

The administrator ("admin" account) can grant the WAN configuration authority to a user ("user" account). If you enable the grant, a user can access **Basic Settings** > **Internet**

Connection menu. For the details for WAN configuration (**Internet Connection** menu), see 4.3.1 PPPoE Configuration on "Internet Connection" Menu.

4.5.3 Backup/Recover Setting

You can back up the configuration, and recover the system with the backed-up config.



You can manage two types of configs; system and WLAN configs.

For each, clicking **Backup** prompts a dialog for saving a config file. You can back up the config to be used for recovering the settings later.

Similarly, clicking **Browse** prompts a dialog for searching a backed-up config. You can specify a config in this dialog, and execute the recovery to the settings with clicking **Recovery**.

i For reflection of recovery, the system reboot is required.

4.5.4 System Reboot

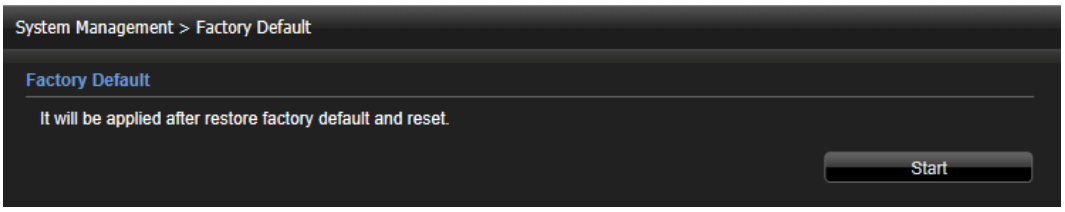
You can reboot the ONT.

Click **Reboot** to restart the ONT system.

i In case that the ONT is assigned IP address by DHCP and the web management is accessed at remote location through the assigned IP address, the reconnection to the web may be failed after a reboot, due to the change of IP address.

4.5.5 Factory Default

You can restore the ONT configuration to the factory default.



If you want to proceed the factory default restore, click **Start**.

If the factory default restore is completed, all of the admin/user settings are deleted. Therefore, it is recommended that you back up the current configuration before proceeding the restore. For the details of config backup, see 4.5.3 Backup/Recover Setting.

i

There are two types of methods to initialize to factory default; **Factory Default** on web (described above) and **RESET** button (positioned as like the figure below). The initialization levels by condition of configuration or physical pushing are as follows:
- **Factory Default** on web by "user" account - Initializes only user-configurable settings.
- **Factory Default** on web by "admin" account - factory default
- Pushing **RESET** for about "10" seconds - Initializes only user-configurable settings.
- Pushing **RESET** for about "30" seconds - factory default