zNID 24xx Series Configuration Guide

For software version 2.5.x
August 2012
Document Part Number: 830-03782-01

ZHONE®

Zhone Technologies
@Zhone Way
7195 Oakport Street
Oakland, CA 94621
USA
510.777.7000
www.zhone.com
info@zhone.com

Zhone Technologies makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability, non infringement, or fitness for a particular purpose.

Further, Zhone Technologies reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Zhone Technologies to notify any person of such revision or changes.

TABLE OF CONTENTS

About This Guide

This guide is intended for use by installation technicians, system administrators, or network administrators. It explains the Web user interface for the zNID 24xx series and how to configure the zNID 24xx series of products.

Style and notation conventions

This document uses the following conventions to alert users to information that is instructional, warns of potential damage to system equipment or data, and warns of potential injury or death. Carefully read and follow the instructions included in this document.

Caution: A caution alerts users to conditions or actions that could damage equipment or data.

Note: A note provides important supplemental or amplified information.

Tip: A tip provides additional information that enables users to more readily complete their tasks.

WARNING! A warning alerts users to conditions or actions that could lead to injury or death.

WARNING! A warning with this icon alerts users to conditions or actions that could lead to injury caused by a laser.

WARNING! This icon warns the user that metal surfaces can become hot to touch. Avoid contact or use caution when touching these surfaces.

Typographical conventions

The following typographical styles are used in this guide to represent specific types of information.

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
`Fixed`	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
`Fixed Bold`	Used in code examples for text typed by users.
`Fixed Bold Italic`	Used in code examples for variable text typed by users.
Italic	Used for book titles, chapter titles, file path names, notes in body text requiring special attention, section titles, emphasized terms, and variables.
PLAIN UPPER CASE	Used for environment variables.

Related documentation

Refer to the following publication for additional information:

- *zNID 24xx Hardware Installation Guide* — explains how to install the zNID, describes the variations of the zNID models in 24xx family, their LEDs and interfaces.
- zNID Quick Installation Instructions — There is a set of Quick Installation Instructions for GPON and GE models which describe in shorter procedures the steps for installing the zNID. These instructions are shipped with the zNID, but are also available on the Zhone website.

Refer to the release notes for software installation information and for changes in features and functionality of the product (if any).

Acronyms

The following acronyms are related to Zhone products and may appear throughout this manual:

Table 1: Acronyms and their descriptions

Acronym	Description
Active E	Active Ethernet, also known as Gigabit Ethernet
APC	Angled physical contact (for fiber connector)
Coax	Coaxial cable
CPE	Consumer Premises Equipment
DHCP server	Dynamic host configuration protocol server
EZ touch	Zhone’s implementation for managing CPEs and zNIDs
GigE	Gigabit Ethernet
GPON	Gigabit passive optical network
HPNA	Home phone line networking alliance
IPTV	Internet protocol TV
LED	Light-emitting diode
MALC	Multi-access line concentrator
MDU	Multiple Dwelling Unit
MIB	Management information bases
MoCA	Multimedia over Coax Alliance
OLT	Optical Line Terminator
OMCI	ONU Management and Control Interface
ONT	Optical Network Terminator
ONU	Optical Network Unit
PoE	Power over Ethernet
PPPoE	Point-to-point protocol over Ethernet
QoS	Quality of service
RF	Radio Frequency
RFoG	Radio Frequency over Glass
SC adaptor	Subscriber connector adaptor
SIP	Session initiation protocol
SNMP	Simple network management protocol

Table 1: Acronyms and their descriptions (Continued)

Acronym	Description
T1/E1	T1 is Trunk line 1 (or DS 1, digital signal level 1). E1 is the European equivalent, though there are a number of differences between the North American T1 and the European E1.
UPC	Ultra physical contact (for fiber connector)
Wi-Fi	Wireless local area network (trademark of Wi-Fi alliance)
VoIP	Voice over IP
zNID	Zhone Network Interface Device
ZMS	Zhone Management System

Technical support

Technical Support for this product is provided by your Internet Service Provider.

Important safety instructions

Read and follow all warning notices and instructions marked on the product and included in the Hardware Installation Guide, available at Zhone.com.

1

zNID 24xx Series

This chapter describes the zNID 24xx. It includes the following sections:

Overview

The zNID 24xx Series (Zhone Network Interface Device) is a family of indoor, full-featured gateways for residential installations. These next generation zNIDs support GPON or Active Ethernet termination to meet the demands of multi-service network deployments to the user.

With either GPON or Active Ethernet uplinks, the 24xx Series zNIDs deliver data, voice, or video (IPTV) over fiber.

The 24xx series of zNIDs share a common software architecture with the 42xx and 9xxx series of zNIDs, including the same intuitive Web interface and command line interface. The zNID can also be managed by the Zhone Network Management System (ZMS) which uses SNMP. Software upgrades and configuration backups can be handled automatically by the ZMS using the EZ Touch management feature.

The zNID is a full-featured gateway supporting services such as DHCP server, rate limiting, filtering, comprehensive logging, and more. The zNID product line implements a very flexible QoS allowing the service provider to guarantee that services are being prioritized correctly and the end-user receives the Quality of Experience that is expected.

All 24xx series Single Family Unit (SFU) ONTs provide the same voice features found on the 42xx series of outdoor residential SFU ONTs and the 9xxx series of Multiple Dwelling Unit (MDU) ONTs. SIP-PLAR signaling is supported for connection via Zhone's Voice Gateway to traditional Class 5 TDM switches, while both MGCP and SIP are supported for direct connection to a VoIP Softswitch. This flexibility allows Zhone's 9xxx, 42xx and 24xx Series ONTs to work in nearly all Telco networks, with interoperability support for a broad array of Softswitches.

Zhone’s GPON ONTs are commonly are used in the 20km range with other GPON ONTs in the distribution network, though can reach up to 60km depending on the configuration of the optical distribution network (ODN).

Zhone's 24xx Active Ethernet ONTs can operate at distances up to 20km.

The zNID enclosure is designed to provide outstanding reliability and simple installation.

The zNID 24xx series may be managed by

- EZ Touch (Zhone's CPE and zNID management application)
- Zhone Management System (ZMS)
- Web (HTTP)
- Command Line Interface (CLI/Telnet/SSH)
- ONT Management Control Interface (OMCI) ***for GPON only***

More information about management capabilities see *Management* on page 19 and *Logging in to the 24xx series zNIDs* on page 29.

For information about special configurations such as Microsoft Media Room and Any Port, Any Service, see *Chapter 4, Special scenarios,* on page 213 for *Microsoft Media Room support* and *Any port, any service*.

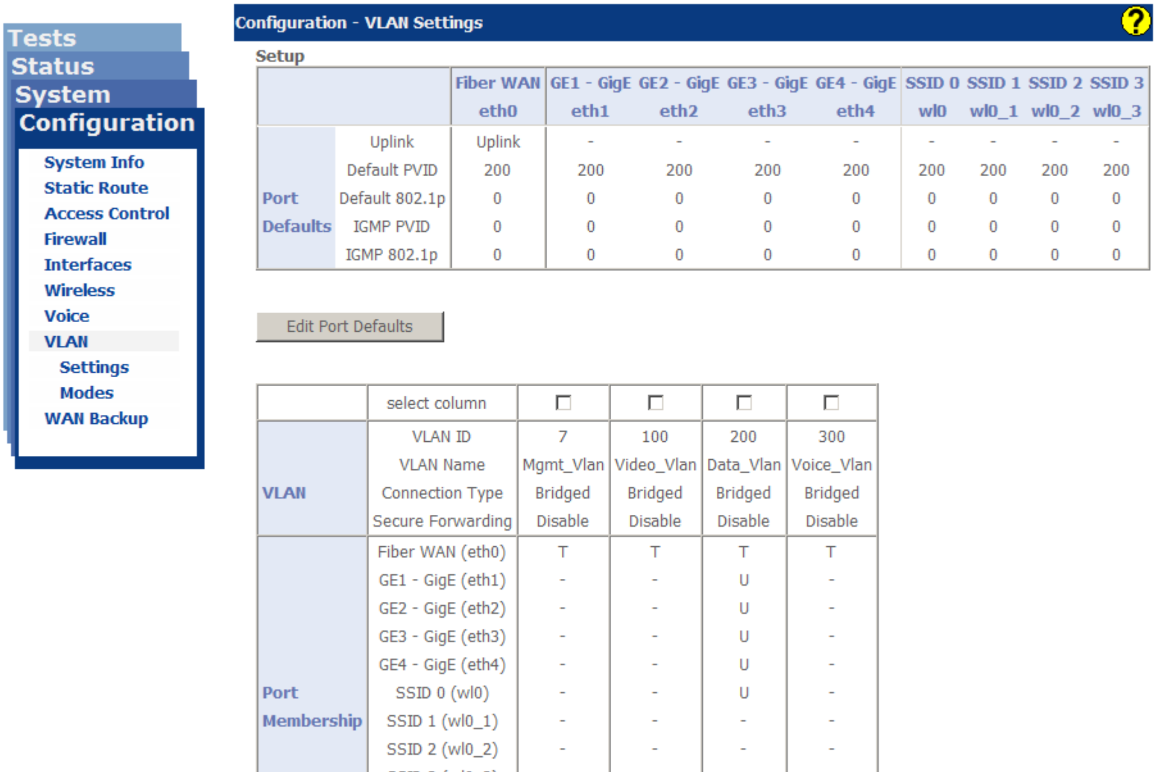
Web user interface

The zNID 24xx data path architecture is VLAN centric. In other words to pass traffic VLANs must be defined. The main page for seeing how the zNID is configured is the **Configuration | VLAN | Settings** page which shows in the lower table the VLANs which have been created and the ports which are members of each VLAN. The type of connection is also displayed in the lower table. The upper table shows the port defaults. Figure 1 shows the default state of the zNID 24xx.

To read the **Configuration | VLAN | Settings** page, see *Factory default VLAN definition* on page 87 and *Edit Port Defaults* on page 145. To understand more about VLAN options, see *VLANS* on page 197.

To create bridged, routed, or PPPoE connections as well as configure Voice interfaces see *Deployment scenarios* on page 156.

Figure 1: The VLAN settings page shows the VLANs and the ports which belong to each VLAN



Configuration - VLAN Settings

Setup

		Fiber WAN	GE1 - GigE	GE2 - GigE	GE3 - GigE	GE4 - GigE	SSID 0	SSID 1	SSID 2	SSID 3
		eth0	eth1	eth2	eth3	eth4	wl0	wl0_1	wl0_2	wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	Default PVID	200	200	200	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0	0

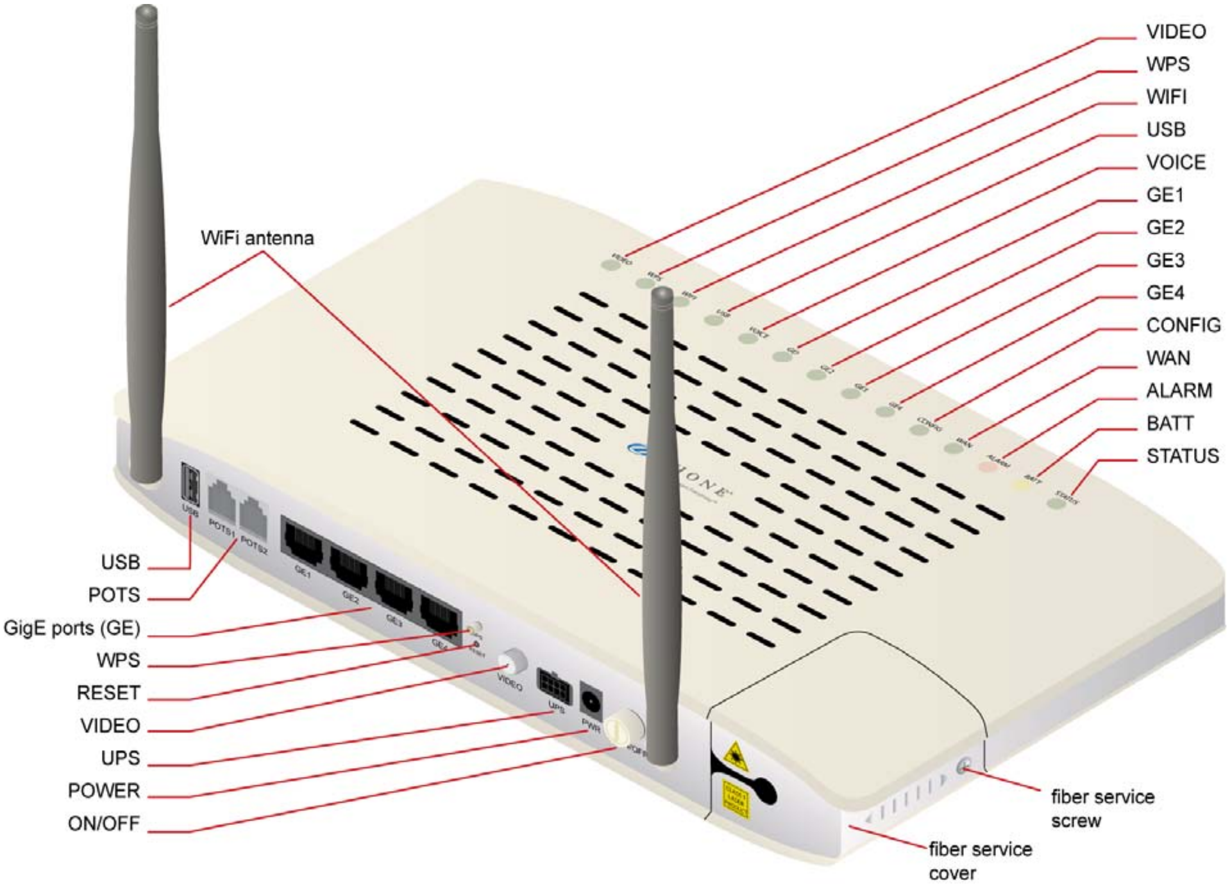
Edit Port Defaults

	select column	□	□	□	□
VLAN	VLAN ID	7	100	200	300
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	Connection Type	Bridged	Bridged	Bridged	Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-
	GE2 - GigE (eth2)	-	-	U	-
	GE3 - GigE (eth3)	-	-	U	-
	GE4 - GigE (eth4)	-	-	U	-
	SSID 0 (wl0)	-	-	U	-
	SSID 1 (wl0_1)	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-

zNID 24xx series components

The zNID 24xx series has models which have either GPON or Gigabit Ethernet interfaces on the WAN side and Gigabit Ethernet ports, POTS, Coax and USB. See the list of *zNID 24xx models and interfaces* on page 17 for information on which models support which interfaces.

Figure 2: The interfaces, displays and buttons for the zNID 24xx



Depending upon the zNID model selected, the interfaces on the zNID can include:

- One, two, or four Gigabit Ethernet RJ45 ports
- Two Phone Ports (POTS)
- One Coax Port with RF Video
- USB port

To reset the zNID 24xx

1. Press a pin into the reset button and hold it down until all LEDs are on together.
2. Release the reset button.

zNID 24xx models and interfaces

GPON models

The zNID 24xx series GPON models have the following interfaces:

Model	Description
zNID-GPON-2402	GPON Uplink, 2 GigE
zNID-GPON-2403	GPON Uplink, 2 GigE, RFV
zNID-GPON-2424	GPON Uplink, 2 POTS, 4 GigE
zNID-GPON-2425	GPON Uplink, 2 POTS, 4 GigE, RFV
zNID-GPON-2426	GPON Uplink, 2 POTS, 4 GigE, WiFi, USB
zNID-GPON-2427	GPON Uplink, 2 POTS, 4 GigE, WiFi, RFV, USB

Gigabit Ethernet models

The zNID 24xx series Gigabit Ethernet models have the following interfaces:

Model	Description
zNID-GE-2402	GE Uplink, 2 GigE
zNID-GE-2424	GE Uplink, 2 POTS, 4 GigE
zNID-GE-2426	GE Uplink, 2 POTS, 4 GigE, WiFi, USB

2 MANAGEMENT

This chapter describes the zNID 24xx. It includes the following sections:

Management interfaces

The zNID 24xx products can be fully managed through any of several methods (CLI, Web, SNMP and OMCI).

The device uses VLAN 7 as the default management VLAN, with DHCP Client enabled. This allows the ONU to automatically obtain an IP address when connected to an MXK.

CLI

The zNID 24xx products can be managed using a command line interface.

Web

The zNID 24xx products can also be fully managed through the web (HTTP) interface. The web pages are very intuitive and they include a context sensitive help button for additional information. The web interface will be used for the configuration examples used in this document.

Note: The web pages will vary slightly depending on model.

SNMP

The zNID 24xx products can also be managed through SNMP. The zNID 24xx family is compatible with any industry standard SNMP agent. However, Zhone provides a CPE manager feature that makes managing the ONUs even easier.

OMCI

ONU Management Control Interface (OMCI) provides policy based configuration and management capabilities for GPON. OMCI management is intergrated into the OLT command set, so configuration of the ONU with OMCI is done from the OLT, not directly as with the Web UI or CLI interfaces. Not all modules in the zNID, such as the wireless interface, can be configured directly from OMCI, however they may be used with OMCI via the Virtual Ethernet Interface Point. See OMCI vs. Residential Gateway management, page 21 for more information.

OMCI vs. Residential Gateway management

For GPON zNIDs, the zNID 24xx may be configured and managed from both OMCI and from a residential gateway interface (CLI or Web UI). When using both methods of management it is important to understand how each method configures traffic flows. OMCI configured data flows are very different from residential gateway data flows.

The zNID-GPON-24xx models support multiple management interfaces, however for the purposes of this discussion, the management interfaces fall into two groups, the OMCI management interface and the RG management interfaces which includes the Web GUI, CLI and SNMP.

OMCI and RG combine for three types of management modes:

- RG only

  The RG architecture utilizes and Etherswitch, supporting MAC address learning and forwarding (ISO layer 2 bridging) as well as routing. This combination of bridging and routing supported by the zNID provides a broad base of routing options. See IP configuration options, page 157 for more information.

  The RG interface supports wireless and VoIP options for SIP, SIP-PLAR and MGCP See Voice, page 134 and Creating voice connections, page 191 for more information about Voice. Most of this document explains the RG Web UI interface.

  RG only mode is also called RG or RG mode.

- OMCI only

  Data flows are handled differently for OMCI configured flows than for the RG flows. For OMCI data flows there is a one to one mapping between the WAN side GEM port and the LAN side UNI port. All packets are ‘cut-through’ the zNID with no MAC address learning or forwarding.

  The wireless interface is not supported by OMCI. However to map WiFi to OMCI there is another type of management which combines RG and OMCI.

  OMCI only mode is also called ONU mode.

- Dual mode: OMCI and RG

  With dual mode management, the downstream LAN interfaces are configured via the RG interface, and mapped to the Virtual Ethernet Interface Point (VEIP). The VEIP is the common interface point between RG features and OMCI-configured filter rules.

  OMCI and RG combined mode always uses the VEIP.

Comparing RG, OMCI and VEIP by service, traffic forwarding

Another way to understand the three GPON interface types is by service and traffic forwarding.

RG

With RG interfaces you can configure all service modules on the zNID 24xx. RG VLANs pass through an integrated Etherswitch and are forwarded based on Destination MAC to any interface, including the integrated Router. Packets are classified on ingress and handled by the integrated Ethernet Switch and CPU routing, voice or WiFi.

RG VLANs use the 5xx GEM exclusively (unless mapped to the VEIP, in Dual Managed mode, in which case any GEM can be used).

See *RG configured flows* on page 22 for more information.

OMCI

OMCI configured ONU flows require a 1:1 UNI:GEM mapping.

OMCI configured ONU flows are cut-through flows with no bridging, no switching, no routing.

WiFi is not supported in OMCI only mode.

Voice can operate as an OMCI-configured function or an RG-configured function.

RG configured flows and OMCI configured flows can co-exist, but Voice must be OMCI-configured. Remember the following rule: OMCI always wins.

See *OMCI configured ONU flows* on page 24 for more information.

Dual Managed

Dual Managed connections mapped to the VEIP connections may use any GEM. In this mode, RG VLANs operate as described above, but instead of using the default 5xx GEM, OMCI is used to configure the GEM and VLAN filter rule.

See *Dual Managed mode using the VEIP* on page 27 for more information.

RG configured flows

RG configured flows are flows configured via an RG management interface: TR-069, Web GUI, Telnet/CLI, or SNMP. This document mainly describes the Web GUI, so we will not go into much detail about the various configurations in this section.

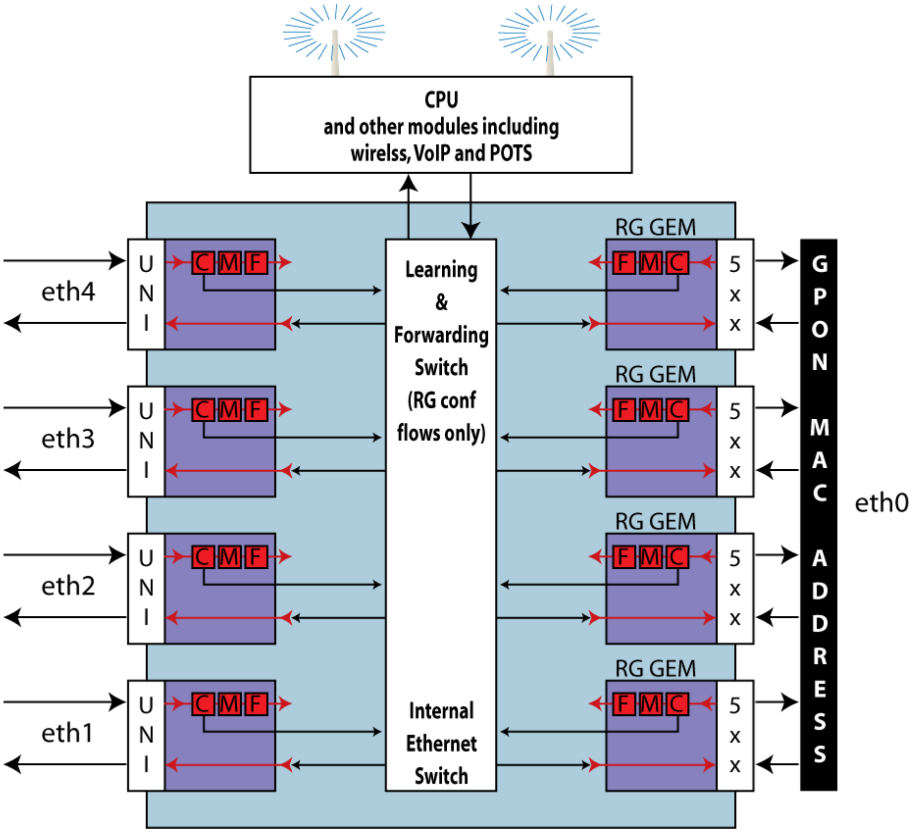
For a discussion of the configurations available and example procedures see Deployment scenarios, page 156 and IP configuration options, page 157.

All services are configured on a per VLAN basis. The RG interfaces can configure data, video, and voice.

for all RG VLANs, an integrated Etherswitch is included in the data forwarding path. This enables RG VLANs to support local Bridging and peer-to-peer communications for LAN client devices such as PCs. Additionally, a Bridge Table is maintained for all Bridged RG VLANs to show learned source MACs per VLAN and per Port.

Packets are classified on ingress, then the learning and forwarding switch determines where to send. See *VLANS* on page 197 for a discussion of layer 2 forwarding behaviors.

Figure 3: Remote Gateway configured flows



GEM ports in the 5xx - 6xx range are reserved for Residential Gateway traffic flows.

By default, all RG VLANs map to the 5xx RG GEM. This mapping is not configurable, and does not require any OMCI provisioning action to create the 5xx GEM on the 24xx unit.

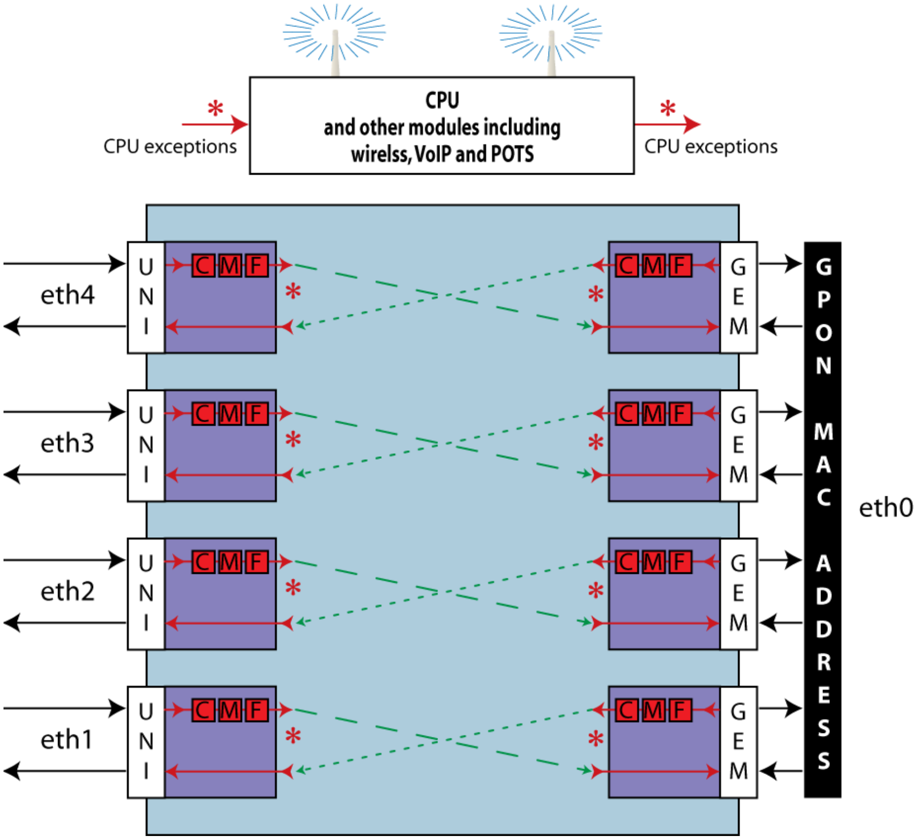
The OLT must not send any OMCI provisioning commands for the 5xx GEM to the 24xx ONT. The reason is that “OMCI always wins.” Whatever provisioning actions that are specified by OMCI commands will occur. If OMCI attempts to provision the 5xx GEM, the 24xx ONT will create the specified ONU traffic flows on the 5xx GEM and disruption to RG traffic flows may occur.

OMCI configured ONU flows

OMCI configured ONU flows have a one to one mapping between the WAN side GEM port (GPON Encryption Method port) and the LAN side UNI (User Network Interface). Other than exception packets which require analysis, such as IGMP joins and leaves or ARPs, the traffic is generally a cut-through between the GEM and the UNI.

OMCI configured ONU flows are handled entirely by Classification, Modification, and Forwarding (CMF) hardware functions. The GPON interface and each Ethernet LAN port of the 24xx have dedicated CMFs. Downstream packets that arrive on each GEM are classified based on the classification rules that have been created by OMCI provisioning actions. Packets that match a Classification Rule are Modified as specified by that rule and Forwarded to the egress port specified by that rule. Packets that are not classified are dropped/blocked. Exception packets that require CPU analysis (like the IGMP joins and leaves or ARPs) are classified on ingress and forwarded to the CPU for action. This ONU forwarding architecture is illustrated in the diagram below.

Figure 4: OMCI configured flows



You cannot map two UNIs to the same GEM when configuring ONU flows. If three Ethernet Ports must be configured as members of the same VLAN for High Speed Internet Access Service, three GEMs are required. The same

VLAN is configured on all three GEMs. When configured this way a PC connected on eth 1 will NOT be able to communicate directly with a PC connected to eth 2 or eth 3. All packets are forwarded upstream in a secure manner, and no locally switched port-to-port communication is supported. All communication between a PC on eth1 and a PC on eth 2 will go upstream to the OLT and back down again.

OMCI unique features

There are some features which OMCI provides which are not provided through the RG:

- VLAN Translation (changing the VLAN tag)
- VLAN Promotion (adding an outer tag)
- VLAN Translation & Promotion (changing the inner tag and adding an outer tag)
- Open Trunk (provisioning a cut-through path from an Ethernet Port to a GEM Port that will pass all traffic through, unmodified, regardless of VLAN ID). This open trunk is a useful feature for business applications where a large number of VLANs must be supported.

OMCI configured video

The IP TV application is fully supported in pure ONU mode. The 4095 GEM is used for all downstream multicast traffic, and the same 1:1 mapping of UNIs to GEMs is required for handling of uni-cast traffic.

VLAN Translation is supported for the IP TV application, as long as all Ethernet Ports are members of the same original VLAN. It is not possible to translate a single downstream multicast video packet to VLAN A for sending out eth 1, while simultaneously translating the same packet to VLAN B for sending out eth 2

OMCI configured voice

The SIP Voice application is fully supported in pure ONU mode. OMCI-configured SIP voice must be mapped to a dedicated GEM. SIP-PLAR and MGCP voice are not supported in ONU mode.

Voice is unique because it is an ISO layer 3 application that can be fully provisioned via OMCI and handled as an ONU function, or it can be fully provisioned via Telnet/CLI, Web GUI, SNMP or TR-069 and handled as an RG function. In either case, Voice actually operates as an RG function. OMCI is used to configure the exact same database parameters for voice that are provisioned via any of the RG configuration interfaces (e.g. Web GUI).

The only difference between ONU Voice and RG Voice is the Bound Interface that is assigned. When Voice is OMCI-configured, the Bound Interface is a “brg” interface created via OMCI. When Voice is RG-configured, the Bound Interface is an IP Interface created via the Web GUI or TR-069.

This display is useful for troubleshooting purposes, because you can easily see how voice is configured using the Web GUI, TR-069, or Telnet/CLI interface, even when OMCI actually configured it.

Statistics in UNI mode

There are not as many packet-level statistics available for ONU flows since they are ISO layer 2 “cut-through” flows as illustrated in OMCI configured flows, page 24. However there are several useful debug tools.

- There is an IGMP Table for OMCI-configured flows, accessible via Telnet/CLI or Web GUI
- Voice Packet Log, Audit Log, and Line Status. Accessible via Telnet/CLI or Web GUI
- Ethernet Port Statistics are provided. Accessible via OMCI, Telnet/CLI or Web GUI
- GPON physical layer statics are provided. Accessible via OMCI, Telnet/ CLI or Web GUI

There is no Bridge Table to show learned MACs for any OMCI configured flows.

Reserved GEM ports

When using any configuration mode:

- GEM ports in the 0xx, 1xx and 2xx range are not supported

  The first usable GEM ports for the 24xx ONTs are in the 3xx - 4xx range.
- GEM ports in the 5xx - 6xx range are reserved for Residential Gateway traffic flows

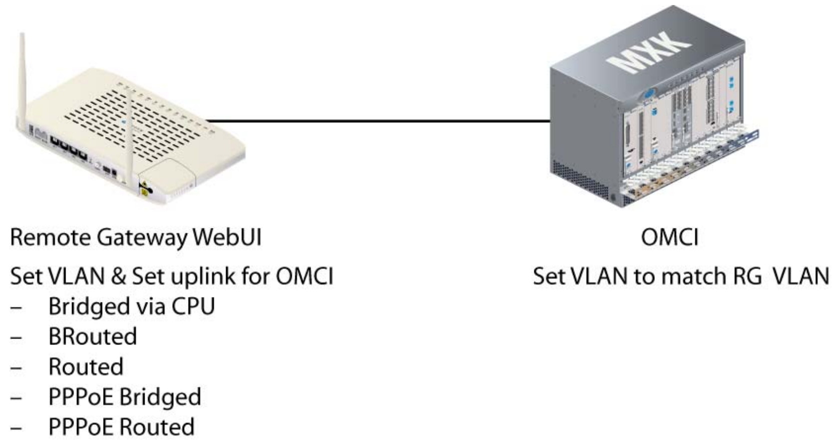
  The “501 - 628 GEM range” is reserved for Residential Gateway VLANs configured via the TR-069 or Web GUI interface. The 2426 uses (501 + ONU ID) as its RG GEM for ONU IDs from 0 to 127.

Dual Managed mode using the VEIP

In Dual Managed mode a “virtual UNI” is the glue between the RG interfaces and OMCI. The virtual UNI is a Virtual Ethernet Interface Point (VEIP) as described in G.984.4 Amendment 2 and G.Impl.984.4).

The VEIP allows the features such as Voice and WiFi which cannot be implemented directly by OMCI, to be configured via RG interfaces. The uplink is then set to “O” to designate an OMCI interface. This mechanism ties the uplink to the virtual UNI.

Figure 5: RG and OMCI in Dual Managed mode, features via VEIP are matched by VLAN Identifier



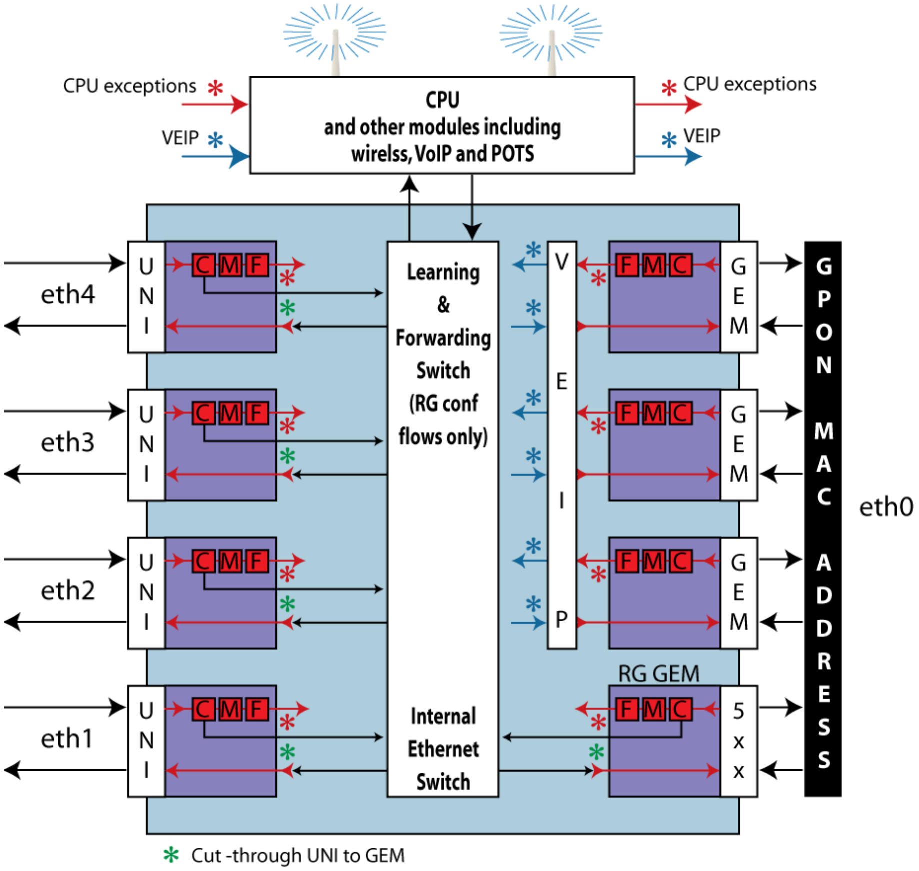
When the eth0 interface of an RG VLAN is configured as an OMCI member, it will be automatically mapped to the VEIP. Conversely, when eth0 is configured as a tagged or untagged member of the VLAN, it is automatically mapped to the default 5xx RG GEM.

Up to 24 RG VLANs are supported, and all 24 of them could be mapped to the VEIP. Each RG VLAN must have a unique VLAN ID. However, VLAN translation rules may be configured via OMCI to map multiple different RG VLANs into the same Network-side VLAN (Not configured on the zNID, but on the OLT).

VEIP Mapping is supported by the following VLAN types: Bridged-CPU, BRouted, Routed, PPPoE-Bridged, PPPoE-Routed.

All IP attributes of an RG VLAN remain under RG configuration control. OMCI is NOT used for provisioning of IP Addresses, DNS Addresses, Subnet Masks, or other IP attributes

Figure 6: In Dual Managed mode, the VEIP provides access to the other modules including the wireless interface



VLAN ID is used to automatically bind the RG VLAN and the OMCI Filter together.

Note: If there are no OMCI Filter Rules provisioned on the VEIP with a matching Original VLAN ID, then the RG VLAN will not have a connection into the network.

The VEIP provides mapping of RG VLANs to one or more additional GEMs, beyond the default 5xx RG GEM. This mapping enables upstream traffic prioritization via GPON Traffic Profile (GTP) parameters on a per-VLAN basis. It also provides VLAN translation and promotion features that are not available for RG VLANs mapped to the default 5xx GEM.

Logging in to the 24xx series zNIDs

There are a few ways to log directly into the 24xx series zNIDs, both out of band and in band.

- Logging in on the Ethernet ports
- Logging in with CLI

Logging in on the Ethernet ports

The zNID 24xx can be managed from the Ethernet ports.

- The ONU has a default IP address of 192.168.1.1 on the Ethernet port. The user can connect a standard PC to the Ethernet port (eth1) and configure the ONU using a standard web browser or telnet session. The PC will need to have an IP address on the same subnet. Typically, 192.168.1.100 is used. Of course, if you change the IP address of the ONU, you will lose connectivity. You would then need to reconfigure your PC to be on the same subnet.
- The default login is “admin” and the default password is “zhone”

☑ **Note:** For security reasons the password should be changed from the default password. To change the password see *User names and passwords* on page 31.

Logging in with CLI

The complete list of CLI commands can be found in the CLI guide located at: www.zhone.com/support/manuals.

```
Login:admin
Password:zhone
ZNID24xx-Router>
```

To log out of the system, enter the logout command:

```
ZNID24xx-Router> logout
```

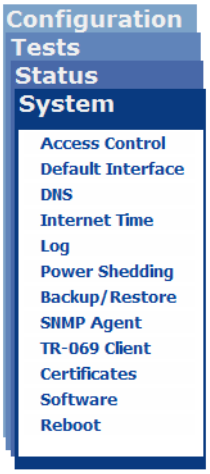
☑ **Note:** For security reasons the password should be changed from the default password. To change the password in the CLI, see the zNID Command Line Interface Reference Guide at zhone.com.

System features

The System pages define and configure access and applications used directly by the zNID, such as DNS and Internet Time. The System pages also provide options for updating and restoring software versions, as well as rebooting the zNID.

For ONUs equipped with POTS there is a power saving feature, power shedding, which cuts power to non-voice services during power outages, so essential voice services may be provided for as long as possible on battery power.

Figure 7: The System menu



This section describes the following System pages:

- *Management access control* on page 31
- *Default interface* on page 33
- *DNS client* on page 34
- *Internet time* on page 37
- *System log* on page 39
- *Power shedding* on page 42
- *Backup/Restore* on page 43
- *SNMP agent* on page 47
- *TR-069 Client* on page 49
- *Certificates* on page 51
- *Restore software* on page 54
- *Update software* on page 55
- *Reboot* on page 56

Management access control

Access to the device is controlled through three user accounts: admin, support, and user. The user name “admin” has unrestricted access to change and view the configuration of the ONU, and to run diagnostics. The user name “support” is used to access the ONU for maintenance and to run diagnostics, however, the support login can not change the configuration. The user name “user” can access the ONU, view a limited subset of the configuration settings and statistics, as well as, update the ONU’s software.

The password can be up to 16 characters.

User names and passwords

Use the fields in the **Access Controls | Password** to enter up to 16 characters and click **Apply/Save** to change or create passwords.

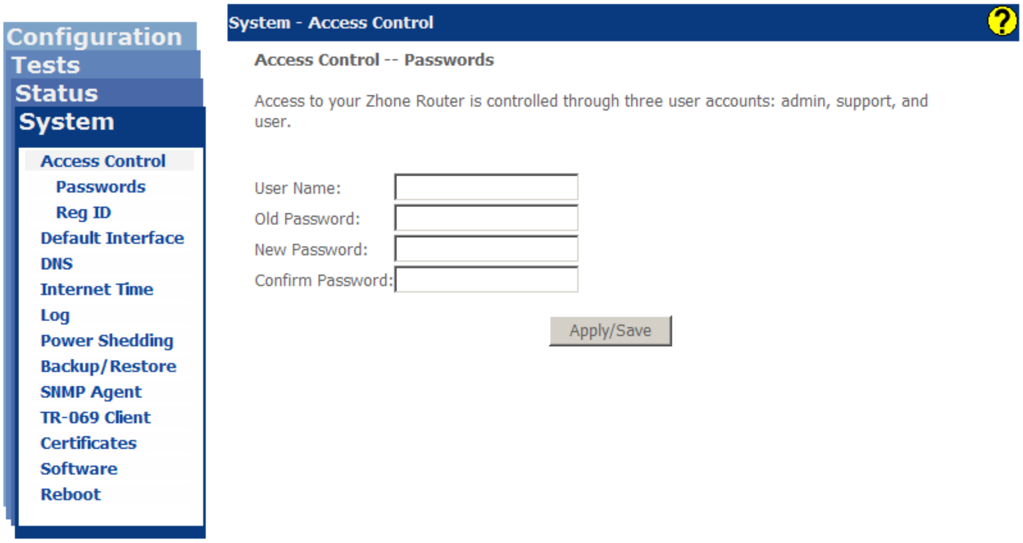
Note: Passwords cannot contain a space.

The user name “admin” has unrestricted access to change and view configuration of your Zhone Router.

The user name “support” is used to access your Zhone Router for maintenance and to run diagnostics.

The user name “user” can access the Zhone Router, view a limited subset of configuration settings and statistics, as well as, update the router’s software.

Figure 8: Access control and changing passwords



System - Access Control

Access Control -- Passwords

Access to your Zhone Router is controlled through three user accounts: admin, support, and user.

User Name:

Old Password:

New Password:

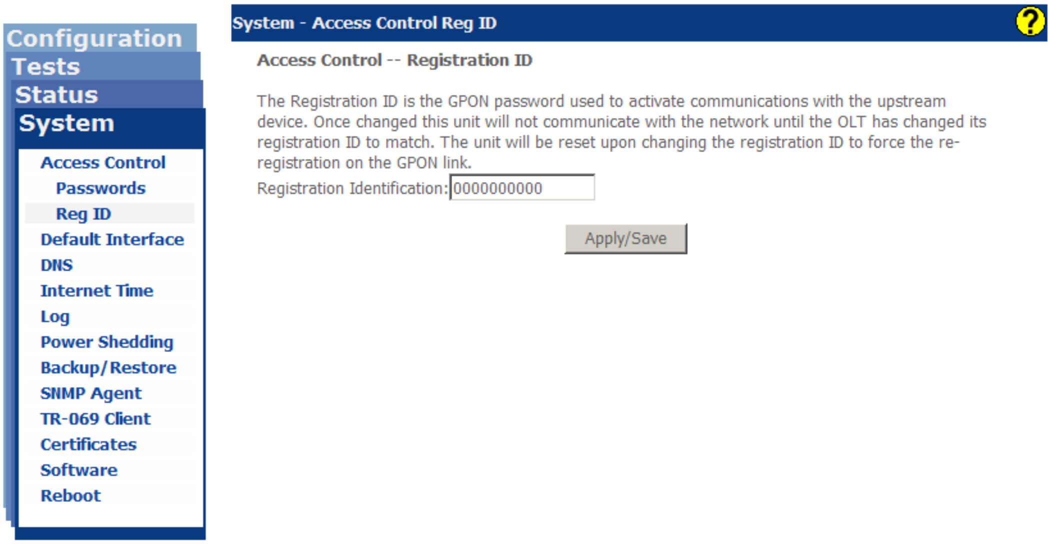
Confirm Password:

Note: For security reasons the password should be changed from the default password.

Registration ID

Access on the GPON interface requires a Registration ID. This value must match the value programmed in the OLT. The system administrator should have programmed this value. Changing the value will disable communications with the network. The unit will reset once the Reg ID has been changed and the GPON link will not communicate with the OLT until the same password is entered in the OLT.

Figure 9: The Registration ID is given from the service provider



Access Control -- Registration ID

The Registration ID is the GPON password used to activate communications with the upstream device. Once changed this unit will not communicate with the network until the OLT has changed its registration ID to match. The unit will be reset upon changing the registration ID to force the re-registration on the GPON link.

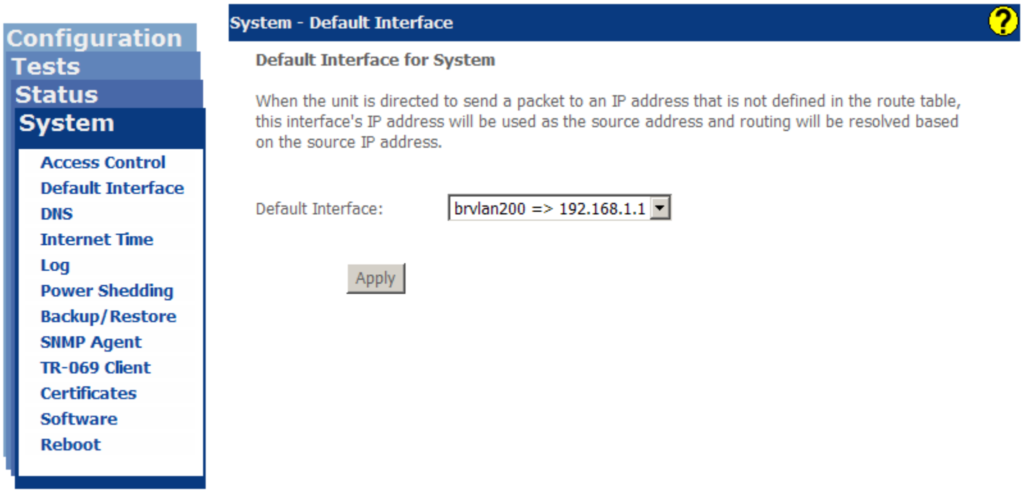
Registration Identification: 0000000000

Default interface

When the ONU must send an internally generated packet (e.g., from SNMP trap, SNTP, etc.) to an IP address that is not defined in the route table, the selected default interface's IP address will be used as the source address.

This device has many internal applications such as SNMP, DHCP, DNS, PING. If one of these applications sends a packet to an IP address which is not defined in the route table and the application has not been directed to use a particular interface to transmit the packet then the default interface's IP address will be used as the source address and routing will be resolved based on that source IP address.

Figure 10: Default interface



System - Default Interface

Default Interface for System

When the unit is directed to send a packet to an IP address that is not defined in the route table, this interface's IP address will be used as the source address and routing will be resolved based on the source IP address.

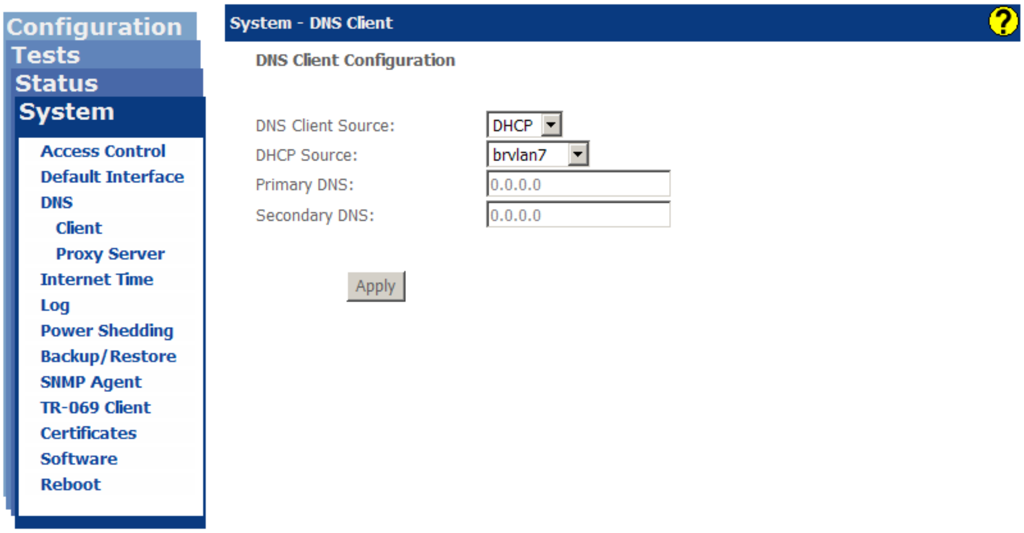
Default Interface: brvlan200 => 192.168.1.1

DNS

DNS client

Depending on the selection of the **DNS Client Source**, you will need to select a source for the DNS, or enter DNS information. Selecting **Static** requires a **Primary DNS** and/or a **Secondary DNS** address to be entered. Selecting any other entry from **DNS Client Source** requires an interface to be selected.

Figure 11: The DNS client screen with DHCP as DNS Client Source



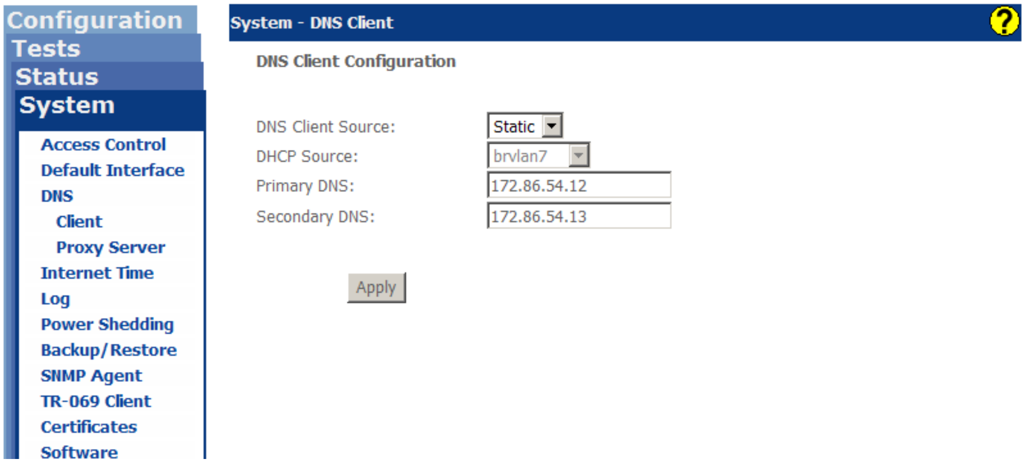
DNS Client Configuration

DNS Client Source: DHCP
DHCP Source: brvlan7
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0

Table 2: DNS client

UI Label	Description
DNS Client Source	• **Static** requires a Primary and/or a Secondary DNS address to be entered. • **DHCP** requires an existing VLAN to be selected as the DHCP source • **PPPoE** requires an existing PPPoE tunnel to be selected as the PPPoE source • **OMCI** The DNS Server IP addresses which are provided via OMCI will be used
Primary DNS	The IP address of the Primary Domain Name Server
Secondary DNS	The IP address of the Secondary Domain Name Server
DHCP Source	Only available when DHCP is selected as the DNS client source. Select from the existing VLANs
PPPoE Source	Only available when PPPoE is selected as the DNS client source. Select from the existing PPPoE tunnels

Figure 12: Static as DNS Client Source

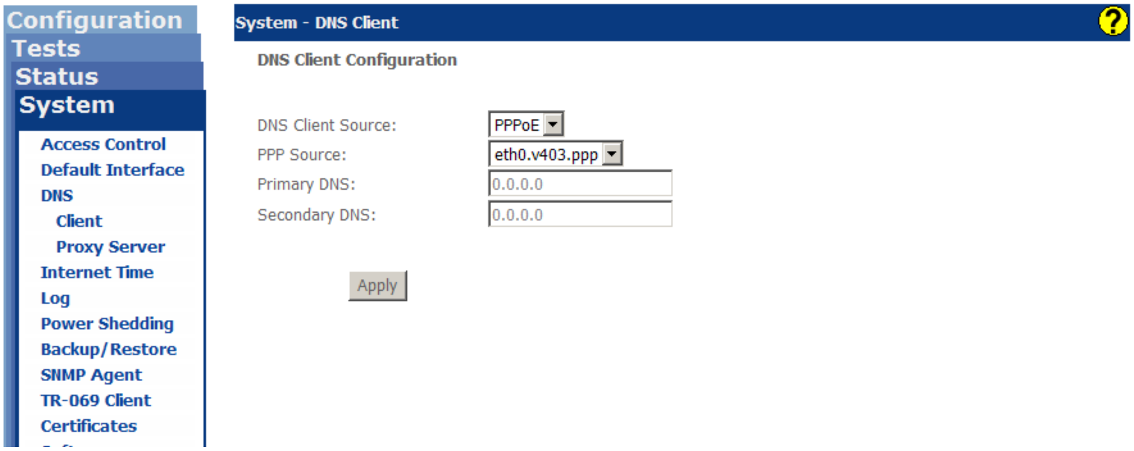


System - DNS Client

DNS Client Configuration

DNS Client Source:	Static
DHCP Source:	brvlan7
Primary DNS:	172.86.54.12
Secondary DNS:	172.86.54.13

Figure 13: PPPoE as DNS Client Source



System - DNS Client

DNS Client Configuration

DNS Client Source:	PPPoE
PPP Source:	eth0.v403.ppp
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0

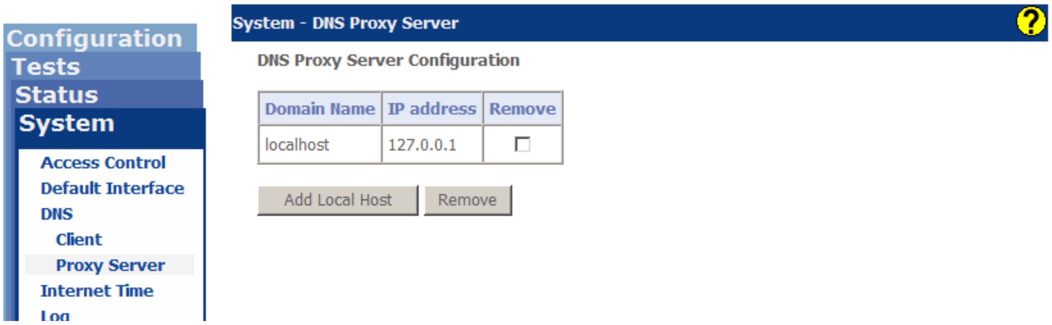
DNS Proxy Server

When DNS Proxy is selected as the DNS Relay Source on any LAN-side interface, client devices will send all DNS requests to this Router LAN side IP Address.

The router checks the Local Host Table for any pre-configured Domain Name lookups, and if a matching entry is found, responds with the corresponding IP Address.

When there are no matching entries in the Local Host Table, the router initiates a Proxy DNS Request using its System DNS Client, then generates a corresponding DNS response to the LAN-side client with the corresponding IP Address learned via the Proxy Request.

Figure 14: Displaying the DNS Proxy Server (default shown)



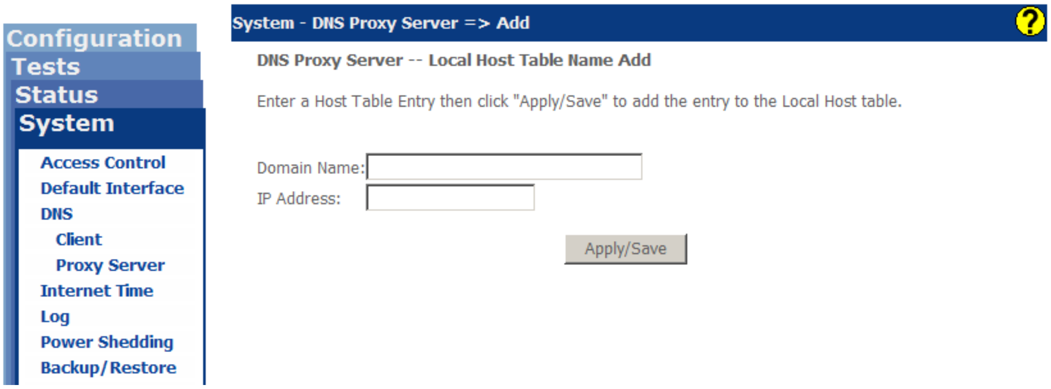
System - DNS Proxy Server

DNS Proxy Server Configuration

Domain Name	IP address	Remove
localhost	127.0.0.1	□

The Host Names of locally attached devices are dynamically learned and automatically populated in the DNS Proxy Table. Domain Names must be statically configured. The entire Domain Name must be configured (e.g. discovery.microsoft.iptv.com) along with the IP Address that should be returned to the local clients to send a DNS Request for that Domain Name.

Figure 15: To add a DNS Proxy Server add the Domain Name and IP address



System - DNS Proxy Server => Add

DNS Proxy Server -- Local Host Table Name Add

Enter a Host Table Entry then click "Apply/Save" to add the entry to the Local Host table.

Domain Name:

IP Address:

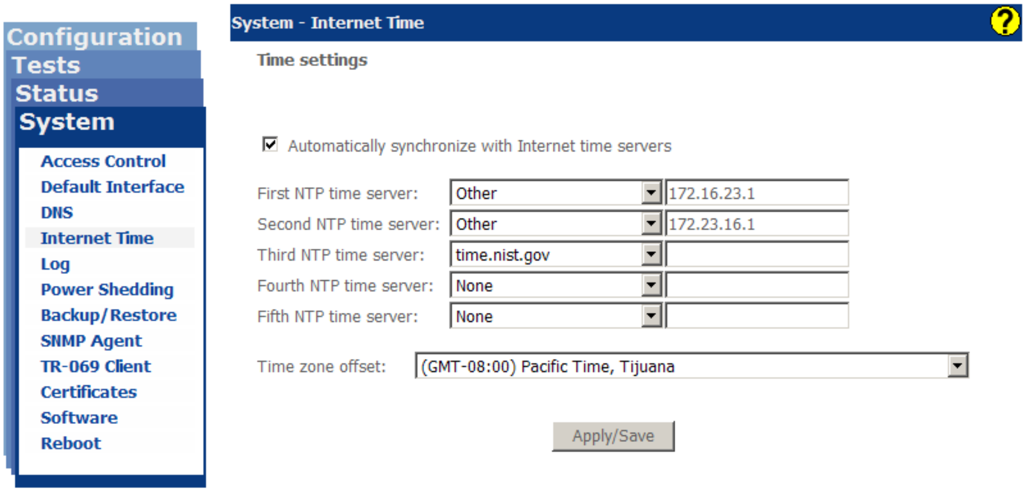
Internet time

The **System|Internet Time** page is used to configure the time of day on the ONU. The time is retrieved from one of the SNTP servers configured on the page. The Time Zone is used to set the time to local time. Note that the ONU does not automatically compensate for Day Light Saving Time.

DHCP Option 42 is supported. If a DHCP offer uses Option 42 to specify an SNTP server and time zone offset, it will automatically configure the SNTP attributes on this screen.

The zNID 24xx maintains the time of day for applications such as Syslog. The time is acquired from one of five specified time servers. If no time server can be found, the system will default to January, 1. The system allows for up to five time servers to be configured. If the first server is unreachable, the ONU will try the next server. If that is not available, it will try the next one, and so on. The configuration of the time client is shown below.

Figure 16: Internet time settings



Time settings

☑ Automatically synchronize with Internet time servers

First NTP time server: Other 172.16.23.1
Second NTP time server: Other 172.23.16.1
Third NTP time server: time.nist.gov
Fourth NTP time server: None
Fifth NTP time server: None

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

Table 3: Internet time settings

UI Label	Description
Automatically synchronize with Internet time servers	This check box enables the Internet time servers. Currently this check box is the only option for setting the time of day.
First NTP time server	Select the first NTP time server to access from the pull-down list, or select **other** and configure the IP address
Second NTP time server	Select the second NTP time server to access from the pull-down list, or select **other** and configure the IP address.

Table 3: Internet time settings

UI Label	Description
Third NTP time server	Select the third NTP time server to access from the pull-down list, or select **other** and configure the IP address.
Fourth NTP time server	Select the fourth NTP time server to access from the pull-down list, or select **other** and configure the IP address.
Fifth NTP time server	Select the fifth NTP time server to access from the pull-down list, or select **other** and configure the IP address.
Time zone offset	Select the GMT offset from the pull-down list.

System log

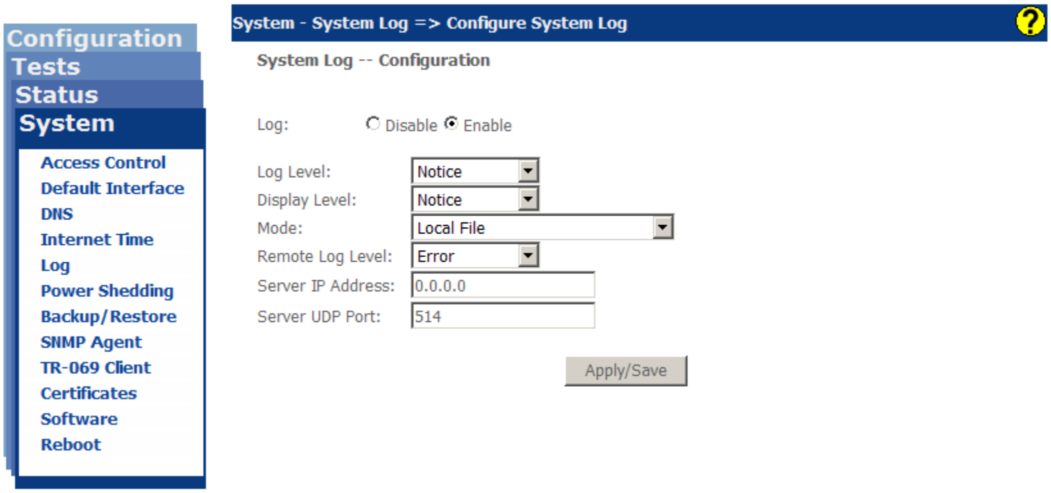
The zNID 24xx supports the system log feature as defined in RFC 5424. The zNID 24xx supports all 8 message severities:

Table 4: System log message severity levels

Message severity	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

The parameter, **Log Level**, determines what messages will be stored in the system log. Any message equal to or greater in priority to the log level setting will be stored in the syslog. The parameter, **Display Level**, determines what messages are displayed on the web or the CLI. The parameter, **Mode**, determines where the messages will be stored. The local messages can be stored in RAM, or they can be stored in a file for later review, or they can be sent to a remote syslog server. Only one remote server is allowed. The priority of the messages is selected by a separate parameter.

Figure 17: Configuring the system log



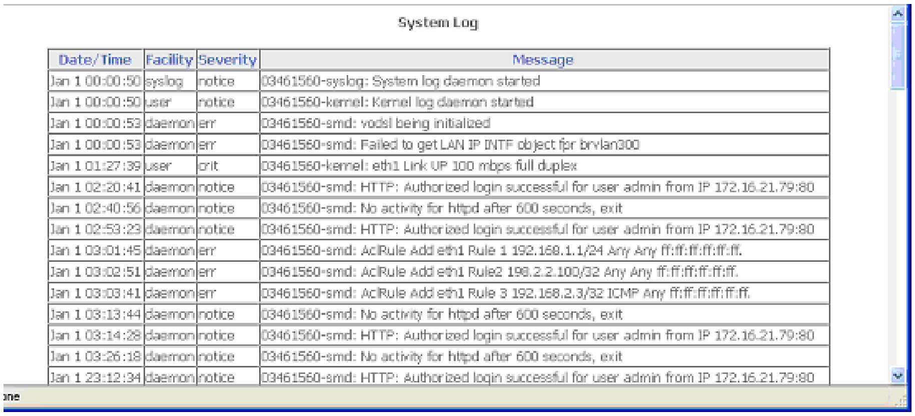
System - System Log => Configure System Log

System Log -- Configuration

Log: ○ Disable ● Enable

Log Level: Notice
Display Level: Notice
Mode: Local File
Remote Log Level: Error
Server IP Address: 0.0.0.0
Server UDP Port: 514

A sample output from the Syslog.



System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:50	syslog	notice	03461560-syslog: System log daemon started
Jan 1 00:00:50	user	notice	03461560-kernel: Kernel log daemon started
Jan 1 00:00:53	daemon	err	03461560-smd: vodsl being initialized
Jan 1 00:00:53	daemon	err	03461560-smd: Failed to get LAN IP INTF object for brvlan300
Jan 1 01:27:39	user	crit	03461560-kernel: eth1 Link UP 100 mbps full duplex
Jan 1 02:20:41	daemon	notice	03461560-smd: HTTP: Authorized login successful for user admin from IP 172.16.21.79:80
Jan 1 02:40:56	daemon	notice	03461560-smd: No activity for httpd after 600 seconds, exit
Jan 1 02:53:23	daemon	notice	03461560-smd: HTTP: Authorized login successful for user admin from IP 172.16.21.79:80
Jan 1 03:01:45	daemon	err	03461560-smd: AclRule Add eth1 Rule 1 192.168.1.1/24 Any Any ff:ff:ff:ff:ff:ff.
Jan 1 03:02:51	daemon	err	03461560-smd: AclRule Add eth1 Rule2 198.2.2.100/32 Any Any ff:ff:ff:ff:ff:ff.
Jan 1 03:03:41	daemon	err	03461560-smd: AclRule Add eth1 Rule 3 192.168.2.3/32 ICMP Any ff:ff:ff:ff:ff:ff.
Jan 1 03:13:44	daemon	notice	03461560-smd: No activity for httpd after 600 seconds, exit
Jan 1 03:14:28	daemon	notice	03461560-smd: HTTP: Authorized login successful for user admin from IP 172.16.21.79:80
Jan 1 03:26:18	daemon	notice	03461560-smd: No activity for httpd after 600 seconds, exit
Jan 1 23:12:34	daemon	notice	03461560-smd: HTTP: Authorized login successful for user admin from IP 172.16.21.79:80

Table 5: Configure system log

UI Label	Description
Log	• Enable Enables the system log function. • Disable Disables the logging of system messages.
Log Level	System Log messages have different priorities. All messages of the selected priority and higher will be placed in the system log. • 0 - Emergency • 1 - Alert • 2 - Critical • 3 - Error • 4 - Warning • 5 - Notice • 6 - Informational • 7 - Debugging
Display Level	Determines the priority level of System Log messages that will be displayed via the GUI, which makes it easy to filter the maximum priority of messages that are viewed.

Table 5: Configure system log

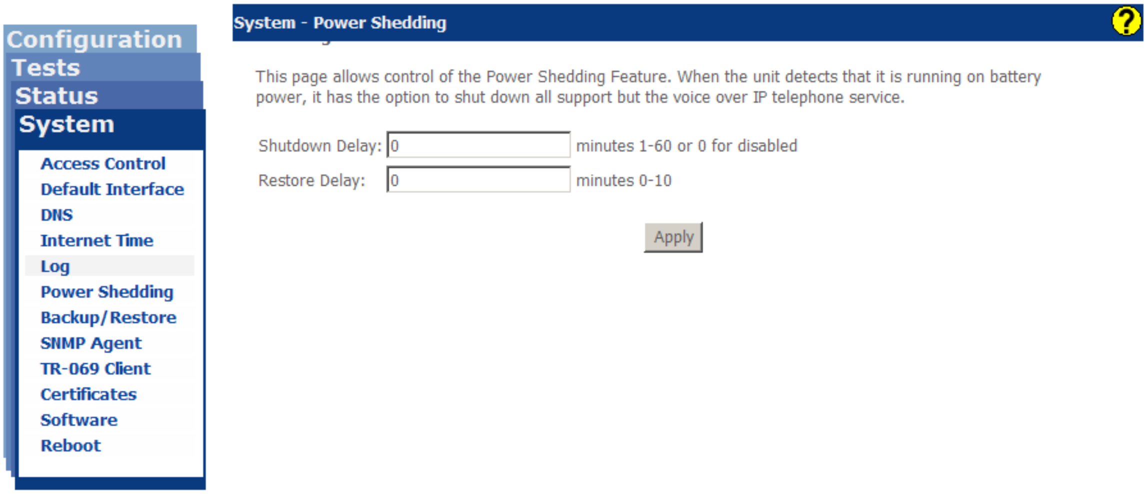
UI Label	Description
Mode	Select where the system log should be recorded • Local Buffer Store Syslog events in local RAM memory • Remote Syslog Send Syslog events to a remote Syslog server • Local Buffer and Remote Syslog Local RAM + remote server • Local File Not currently supported • Local File and Remote Syslog Not currently supported
Server IP Address	If remote - IP address of the Remote Log Server
Server UDP Port	If remote - the UDP port for the syslog protocol. Default is 514

Power shedding

In order to extend telephone service during power outages, so emergency contact may be made for as long as possible on battery power, power shedding may be used to shut down all other services of the ONU. While power shedding is active, all data services will be disabled and only the alarm and system status LEDs will be lit.

Note: The power shedding feature is only activated when a UPS is connected to power the ONU and signals from the UPS indicate that the ONU is actually being powered from the battery.

Figure 18: Configuring power shedding



System - Power Shedding

This page allows control of the Power Shedding Feature. When the unit detects that it is running on battery power, it has the option to shut down all support but the voice over IP telephone service.

Shutdown Delay: 0 minutes 1-60 or 0 for disabled

Restore Delay: 0 minutes 0-10

Table 6: Power shedding options

UI Label	Description
Shutdown Delay	Shutdown delay defines the amount of time in minutes the ONU waits after an AC power outage (which will force the ONU to battery power) before shutting down non-voice services.
Restore Delay	Restore delay determines the amount of time in minutes the ONU will wait after AC power is restored before reactivating non-voice services.

Backup/Restore

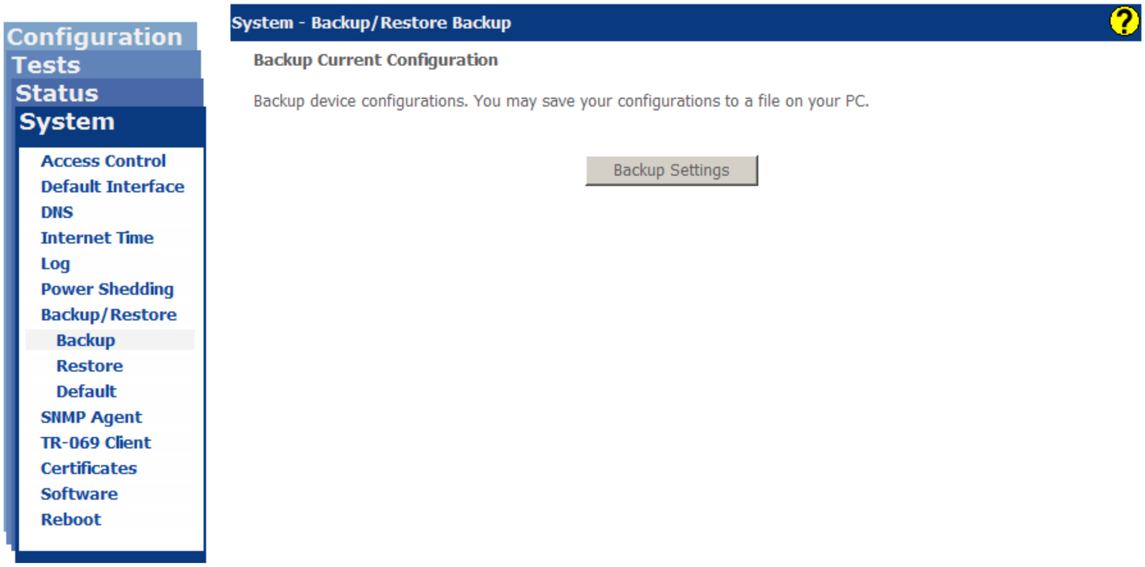
The **Backup/Restore** pages provide the means for backing up the current configuration, restoring earlier configurations, or going back the default settings of the zNID.

Backup

The **Backup/Restore | Backup** screen allows you to save a backup configuration.

Clicking **Backup Settings** on the **System|Backup/Restore|Backup** page will cause the current configuration to be saved on your PC. The configuration is saved under the file name “backupsettings.conf” in a folder determined by your browser’s download settings. It is strongly suggested that filename be changed to more meaning full name that contains the date, or the IP address or the system name of the ONU. Appropriate naming of the file will be critical if you are managing more than one ONU since all the devices will save their configuration under the same filename.

Figure 19: Backup current settings

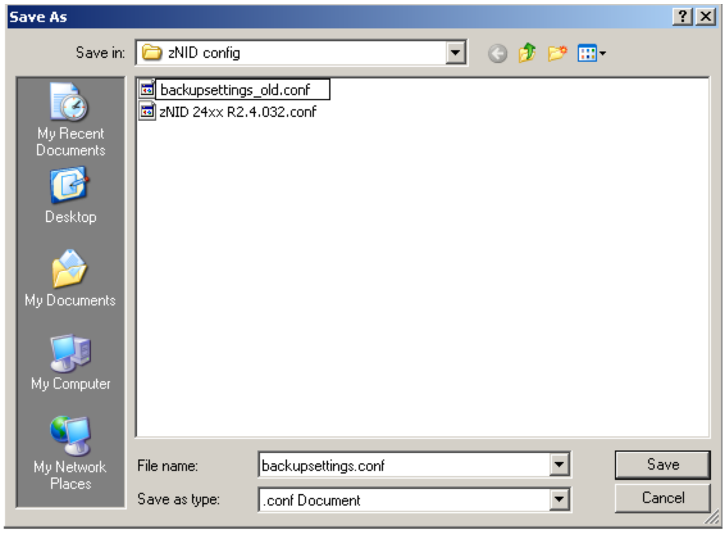


System - Backup/Restore Backup

Backup Current Configuration

Backup device configurations. You may save your configurations to a file on your PC.

Figure 20: Saving the backup configuration file



Save As

Save in: zNID config

backupsettings_old.conf

zNID 24xx R2.4.032.conf

File name: backupsettings.conf

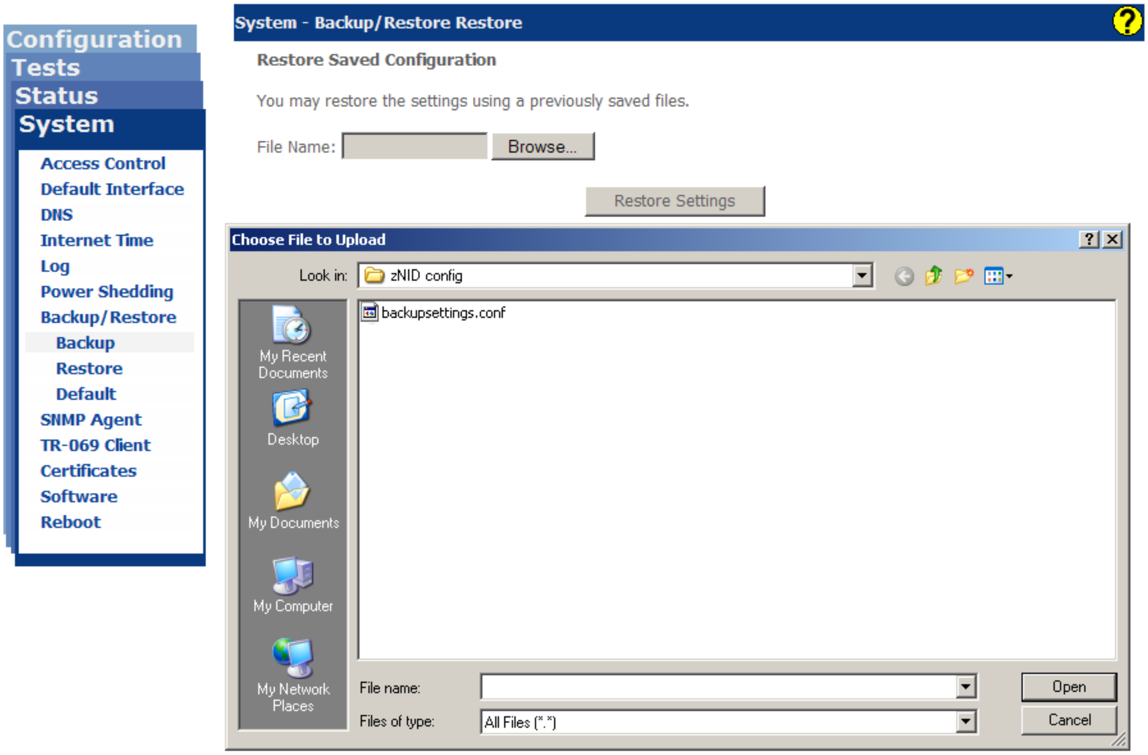
Save as type: .conf Document

Restore

The **Backup/Restore | Restore** screen allows you to restore the ONU to a operate with a previously-saved configuration.

Click **Browse** in the **Backup/Restore | Restore** screen, then select the saved configuration and click open.

Figure 21: Restoring from a saved configuration



System - Backup/Restore Restore

Restore Saved Configuration

You may restore the settings using a previously saved files.

File Name:

Choose File to Upload

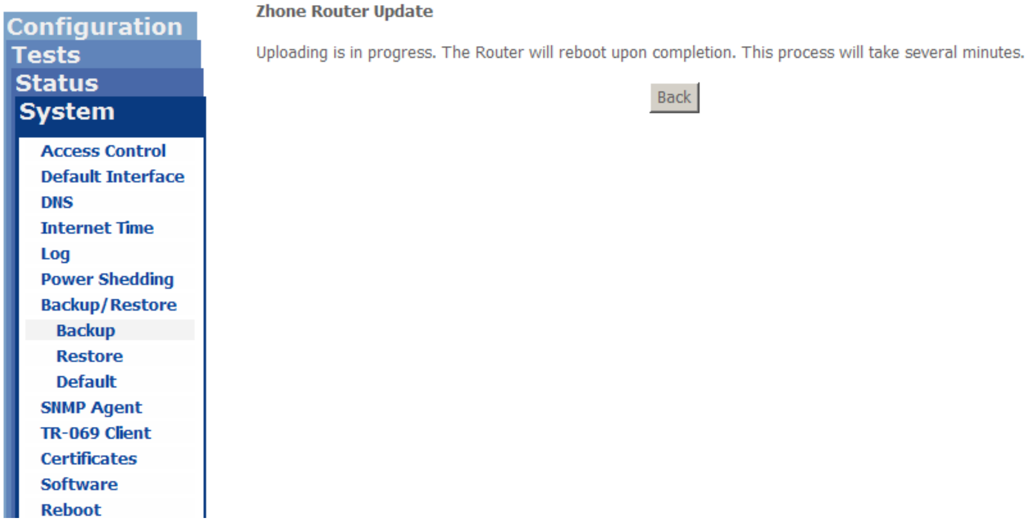
Look in: zNID config

backupsettings.conf

File name:

Files of type: All Files (*.*)

Figure 22: Waiting while the router is being updated



Zhone Router Update

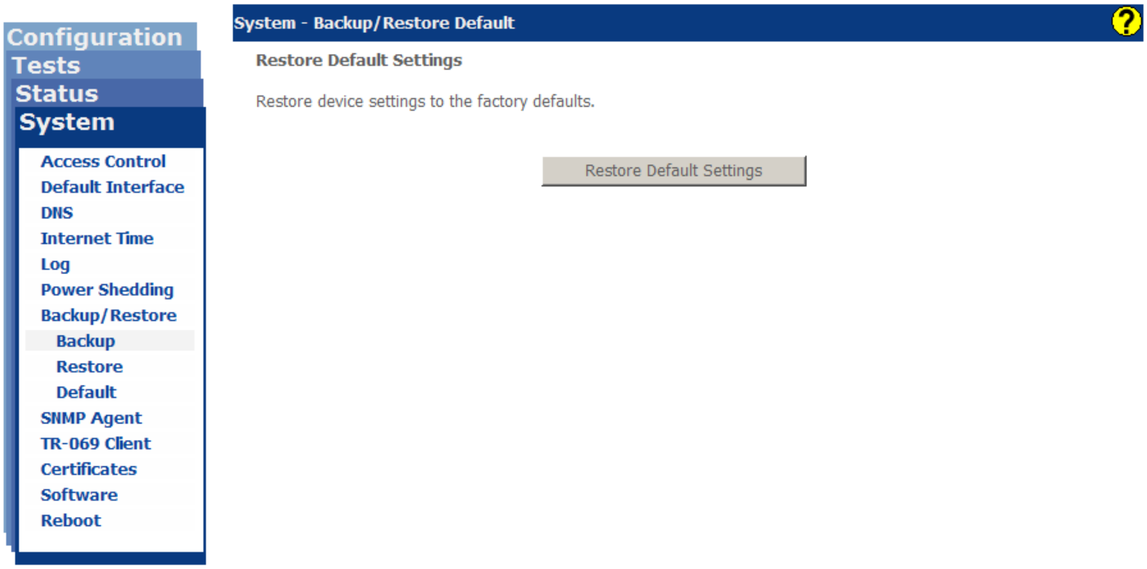
Uploading is in progress. The Router will reboot upon completion. This process will take several minutes.

Restore default

The **Backup/Restore | Restore Default** screen allows you to return to the zNID factory default configuration.

Click **Restore Default Settings**, close the browser window and wait for the router to reboot. If the IP address had been changed from the default IP address you will need to follow the log in directions, *Logging in to the 24xx series zNIDs* on page 29.

Figure 23: Restoring to the factory defaults



System - Backup/Restore Default

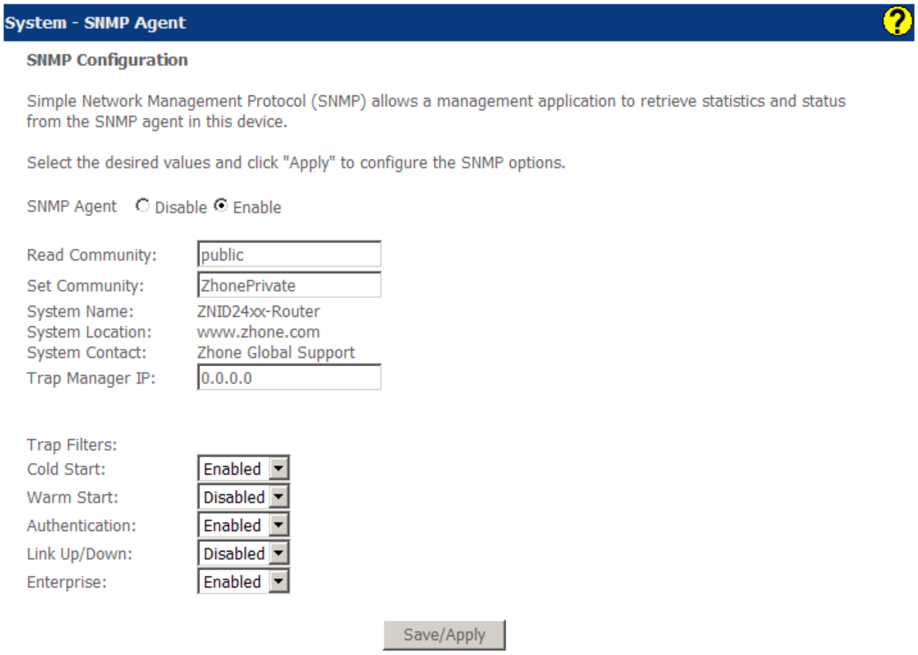
Restore Default Settings

Restore device settings to the factory defaults.

SNMP agent

The **System | SNMP Agent** page allows you to configure the embedded SNMP agent and trap manager. The SNMP agent can be disabled to prevent access from unknown users.

Figure 24: SNMP configuration



System - SNMP Agent

SNMP Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ○ Disable ● Enable

Read Community:	public
Set Community:	ZhonePrivate
System Name:	ZNID24xx-Router
System Location:	www.zhone.com
System Contact:	Zhone Global Support
Trap Manager IP:	0.0.0.0

Trap Filters:

Cold Start:	Enabled
Warm Start:	Disabled
Authentication:	Enabled
Link Up/Down:	Disabled
Enterprise:	Enabled

Table 7: SNMP agent configurable attributes

UI Label	Description
SNMP Agent	• **Enable** Enables the SNMP function • **Disable** Disables the SNMP Feature. The ONU will not send traps or respond to set or get messages.
Read Community	Enter the read community name in the input box. This allows read access from SNMP clients. This field is 32 characters in length, and defaults to “public”.
Set Community	Enter the write community name in the input box. This allows read/write access from SNMP clients. This field is 32 characters in length, and defaults to “ZhonePrivate”.
System Name	Name of this device. The system name will appear in the title bar of the browser. This is a read only field on this page. **System Name** can be set in System info, page 90.

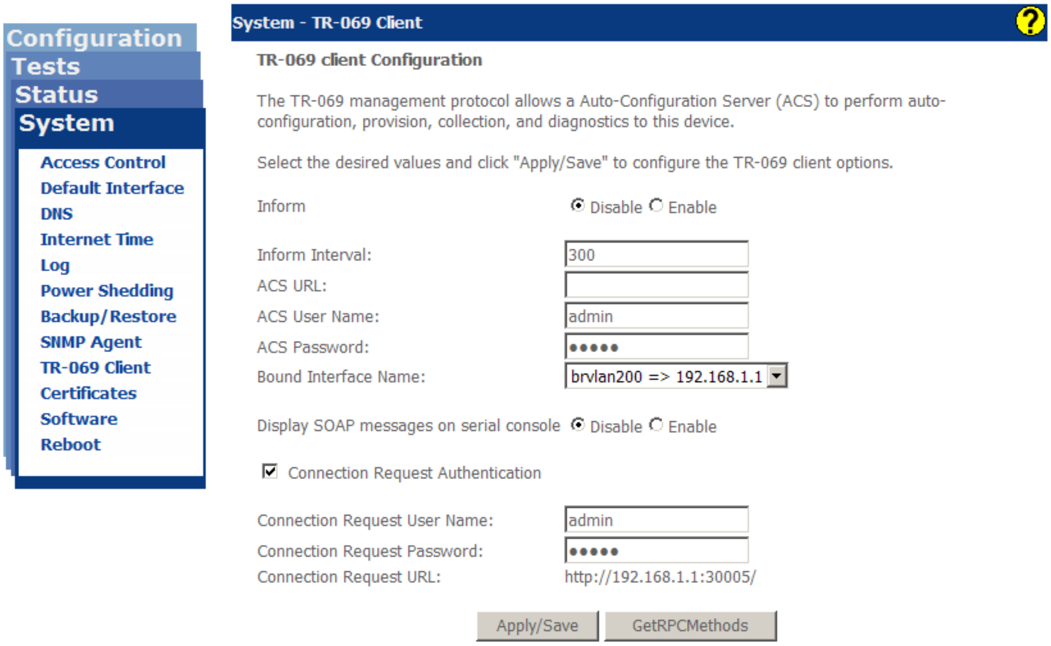
Table 7: SNMP agent configurable attributes

UI Label	Description
System Location	Identifies where this device resides. It could a be a street address or a rack/shelf/slot description. This is a read only field on this page. **System Location** can be set in System info, page 90.
System Contact	The person responsible for this device This is a read only field on this page. **System Contact** can be set in System info, page 90.
Trap Manger IP	The IP address where traps are sent. Currently there is only 1 trap manager allowed.
Trap Filters	The following are a list of SNMP Traps. When Disable the traps will not be sent: • Cold Start The ONU was Powered Off and On • Warm Start The software was rebooted • Authentication Trap Three failed attempts in a row try to log into the box • Link Up/Down Trap A physical interface lost connectivity to its remote peer • Enterprise Trap All non-standard traps will be filtered when set to Disabled. Enterprise traps include Configuration-Change traps, Battery-alarm traps, CPE-Config-Manager traps.

TR-069 Client

The zNID 24xx includes a TR-069 client. TR-069 is a management protocol which allows an Auto-Configuration Server (ACS) to auto-configure, provision, and provide diagnostics.

Figure 25:



System - TR-069 Client

TR-069 client Configuration

The TR-069 management protocol allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	● Disable ○ Enable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	●●●●●
Bound Interface Name:	brvlan200 => 192.168.1.1
Display SOAP messages on serial console	● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name:	admin
Connection Request Password:	●●●●●
Connection Request URL:	http://192.168.1.1:30005/

Table 8: TR-069 client configurable attributes

UI Label	Description
Inform	**Enable** or **Disable** the generation of Inform messages to the ACS.
Inform Interval	Periodic interval (in seconds) at which Inform messages will be generated.
ACS URL	Web site address of the ACS (e.g. http://zhone.com:6050). If the URL includes a domain name, a DNS must be reachable to resolve the domain name.
ACS User Name	User name required to access the ACS.
ACS Password	ACS Password:User password required to access the ACS.
Bound Interface Name	Select the name of an interface to be used for communicating with the ACS.
Display SOAP messages on serial console	**Enable** or **Disable** the logging of Simple Object Access Protocol (SOAP) messages to the serial console and file system.

Table 8: TR-069 client configurable attributes

UI Label	Description
Connection Request Authentication	Check the box to enable the authentication of all Connect Requests received from an ACS. If checked, the TR-069 client will only accept Connect Requests from an ACS that has embedded the correct Connection Request User Name and Password.
Connection Request User Name	User name required to authenticate an ACS Connect Request message.
Connection Request Password	Password required to authenticate an ACS Connect Request message.
Connection Request URL	Connect Request source address used when responding to an ACS Connect Request message. This field is not configurable.
GetRPCMethods	Sends an RPCMethod message to the configured ACS.

Certificates

The zNID 24xx supports local certificates and trusted certificates.

- *Local certificates*
- *Trusted CA*

Table 9: Attributes for Certificates Local and Certificates Trusted CA screen

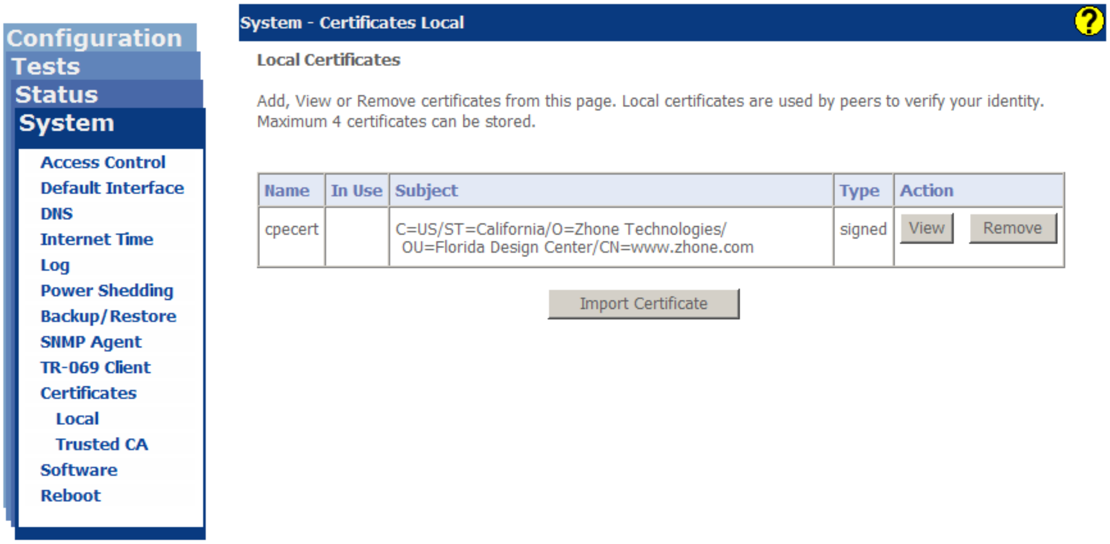
UI Label	Description
Name	Certificate identifier. Local certificate “cpecert” and Trusted CA “acscert” names are reserved for use by the TR069 client.
In Use	“Yes” indicates the certificate has been loaded by the system.
Subject	The person or entity identified within the certificate. The subject content may include: • C (Country code) • S (State) • L (Locality) • O (Organizational Name) • OU (Organizational Unit Name) • CN (Common Name) • email address
Type	Certificate types are request, signed or ca. A certificate request is one that has not been signed by a Certificate Authority (CA). A signed certificate is one that has been signed and may be used to verify the identity of the device with a peer. A ca certificate is a Certificate Authority's certificate that is used to verify your peer's identity without having to contact the CA directly.
Action	View or Remove. Note, removing a certificate that is in use may disrupt services that may be utilizing this certificate.
Import Certificate	Imports a signed certificate to be used as a Local certificate/Trusted CA (depending on which screen) for the system.

Local certificates

Local certificates are used by peers to verify your identity when establishing a connection to a server or client over the secure socket layer (SSL).

The **System|Certificates Local** screen allows you to add, view or remove Local certificates for the system. A maximum of four Local certificates can be stored.

Figure 26: The Certificates Local screen



System - Certificates Local

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

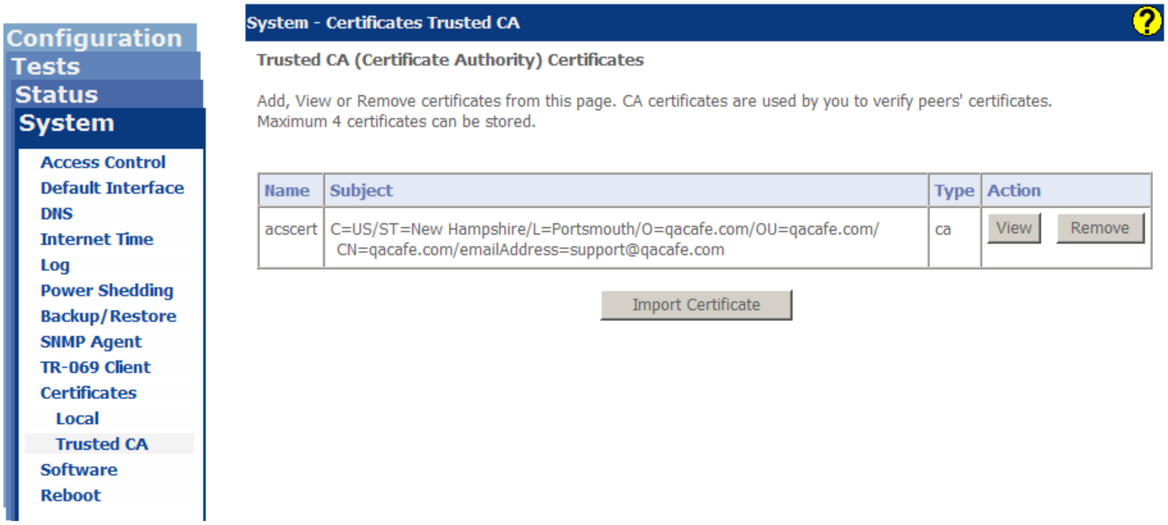
cpecert		C=US/ST=California/O=Zhone Technologies/
		OU=Florida Design Center/CN=www.zhone.com
			signed	View Remove

Trusted CA

Trusted Certificate Authority (CA) certificates are used to verify peer's identity when establishing a connection to a server or client over the secure socket layer (SSL).

The Certificates|Trusted CA screen allows you to import or view Trusted CA certificates for the system. A maximum of four Trusted CA certificates can be stored.

Figure 27: The Certificates Trusted CA screen



System - Certificates Trusted CA

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
acscert	C=US/ST=New Hampshire/L=Portsmouth/O=qacafe.com/OU=qacafe.com/ CN=qacafe.com/emailAddress=support@qacafe.com	ca	View Remove

Import Certificate

Software

The Software screens provide options to restore software from the alternate bank or to use a version of software saved elsewhere.

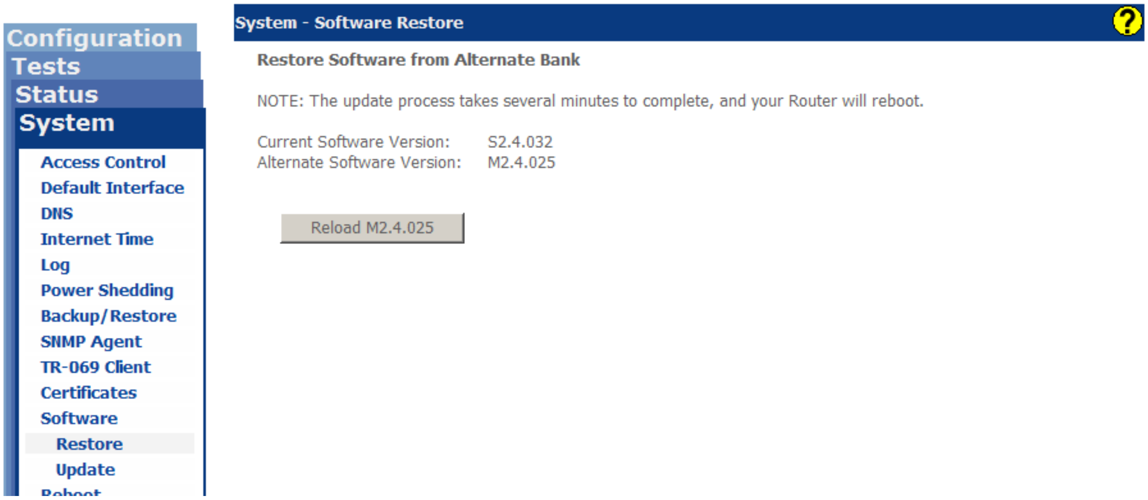
Restore software

The ONU stores two sets of software. One set, the **Current Software Version** or active software, is the software set which is currently running the ONU. The other set is the **Alternate Software Version** or standby software, and is stored in the ONU's alternate (non-running) bank. Clicking **Reload** will cause the alternate software to run the ONU after rebooting it, thus it becomes the current software. The previously current software will then become the alternate software. After the ONU reboots the system will update its display of current and alternate Software versions automatically.The configuration remains unchanged. In other words you do not need to reconfigure the ONU after completing the restore procedure.

Clicking **Reload** software will cause the unit to reboot as it switches to the newly active software. This will happen immediately after clicking — no extra warning message is provided.

Note that when restoring an older version there can be issues with the older code running with a newer configuration data base. The configuration database stores the configuration of the interfaces (with all the services, such as tagging and rate limiting, as well as other configuration information). In some cases, the ONU will have to reset to factory defaults, and then the ONU will need to be manually re-configured.

Figure 28: Restoring software from an alternate bank



Restore Software from Alternate Bank

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

Current Software Version: S2.4.032
Alternate Software Version: M2.4.025

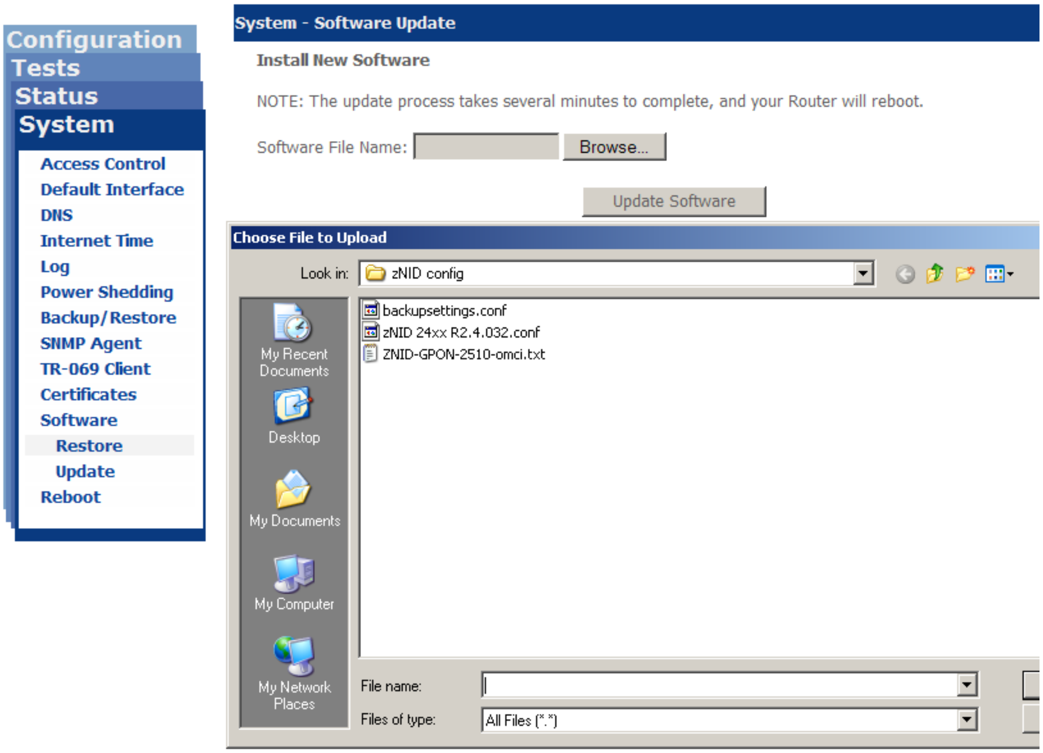
Update software

The ONU may use a saved configuration.

Click **Browse** to view the file system attached to your browser's PC. Then select the configuration file that you would like to use to upgrade the ONU. Clicking **Update Software** will cause the software on the ONU to be updated with the selected software image. The ONU will then reboot.

The ONU will verify that the software image is of the appropriate type, and will reject the file if it is not compatible.

Figure 29: Updating software



System - Software Update

Install New Software

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

Software File Name:

Choose File to Upload

Look in: zNID config

- backupsettings.conf
- zNID 24xx R2.4.032.conf
- ZNID-GPON-2510-omci.txt

File name:

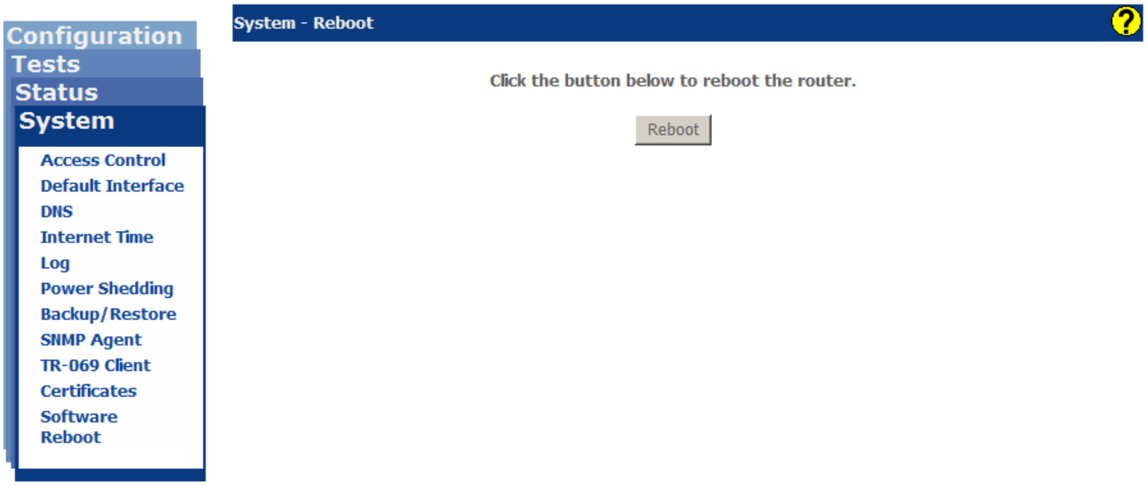
Files of type: All Files (*.*)

Reboot

Clicking Reboot will cause the unit to re-initialize as if it was power cycled. This will happen immediately after clicking — no extra warning message is provided.

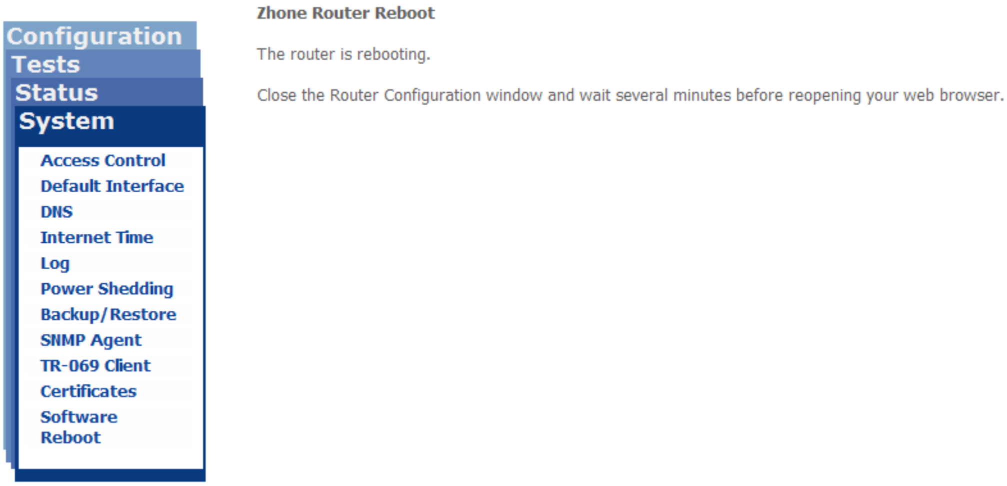
Close the browser window and wait to reconnect to the router.

Figure 30: Rebooting the zNID



Click the button below to reboot the router.

Figure 31: Rebooting message



Zhone Router Reboot

The router is rebooting.

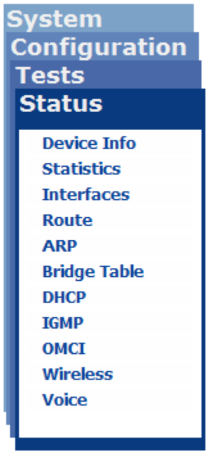
Close the Router Configuration window and wait several minutes before reopening your web browser.

Status and statistics

Status and statistics are very useful in troubleshooting network issues. The zNID 24xx provides

- *Device info* on page 58
- *Statistics* on page 61
- *LAN interface status* on page 65
- *GPON interface status* on page 66
- *PPPoE status* on page 68
- *Route* on page 69
- *ARP table* on page 70
- *Bridge table* on page 71
- *DHCP status* on page 72
- *IGMP* on page 73
- *OMCI* on page 74
- *Wireless* on page 78
- *Voice* on page 79

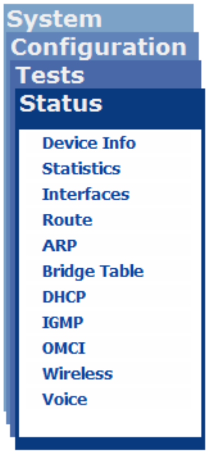
Figure 32: The Status menu

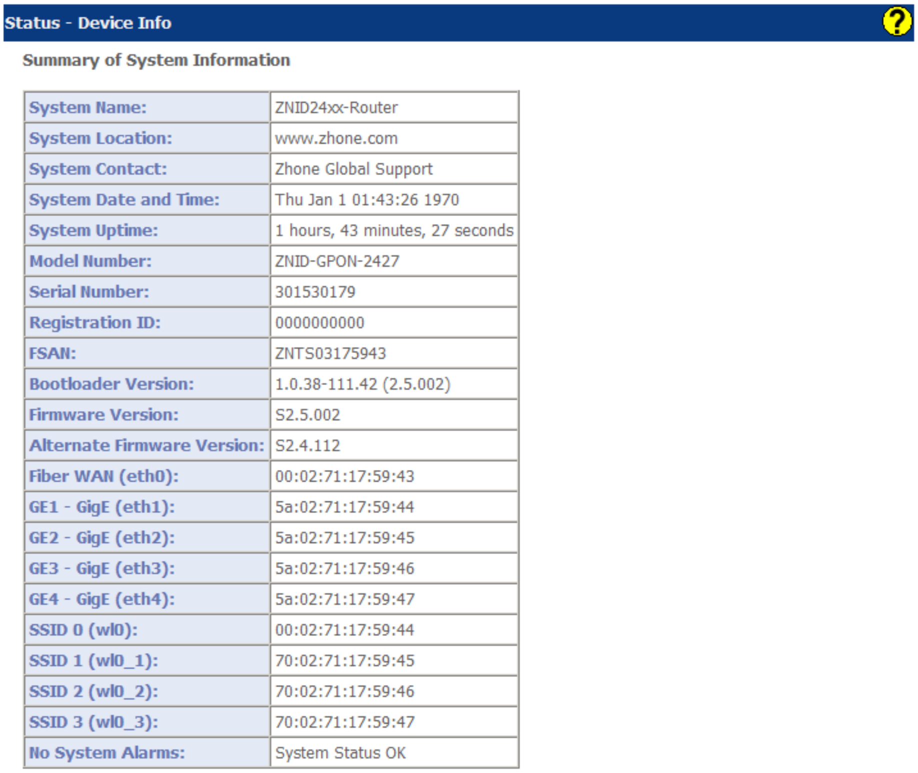


Device info

Device Info includes information about the device, MIB-2 objects, system up time, model number, serial number, version information and the MAC addresses of the interfaces.

Figure 33: The Device Info table





Summary of System Information

System Name:	ZNID24xx-Router
System Location:	www.zhone.com
System Contact:	Zhone Global Support
System Date and Time:	Thu Jan 1 01:43:26 1970
System Uptime:	1 hours, 43 minutes, 27 seconds
Model Number:	ZNID-GPON-2427
Serial Number:	301530179
Registration ID:	0000000000
FSAN:	ZNTS03175943
Bootloader Version:	1.0.38-111.42 (2.5.002)
Firmware Version:	S2.5.002
Alternate Firmware Version:	S2.4.112
Fiber WAN (eth0):	00:02:71:17:59:43
GE1 - GigE (eth1):	5a:02:71:17:59:44
GE2 - GigE (eth2):	5a:02:71:17:59:45
GE3 - GigE (eth3):	5a:02:71:17:59:46
GE4 - GigE (eth4):	5a:02:71:17:59:47
SSID 0 (wl0):	00:02:71:17:59:44
SSID 1 (wl0_1):	70:02:71:17:59:45
SSID 2 (wl0_2):	70:02:71:17:59:46
SSID 3 (wl0_3):	70:02:71:17:59:47
No System Alarms:	System Status OK

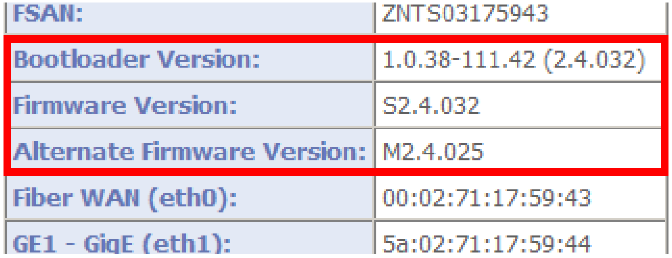
Table 10: Device Info page display

UI Label	Description
System Name	**System Name** is a user definable name which can be used to identify the ONU. **System Name** can be set in System info, page 90.
System Location	**System Location** is user definable information to help identify the ONU and the location of the ONU. **System Location** can be set in System info, page 90. **System Location** is the MIB-2 object, sysLocation.
System Contact	**System Contact** is user definable information to help identify the ONU and who to contact about the system. **System Contact** can be set in System info, page 90. **System Contact** is the MIB-2 object, SysContact

Table 10: Device Info page display

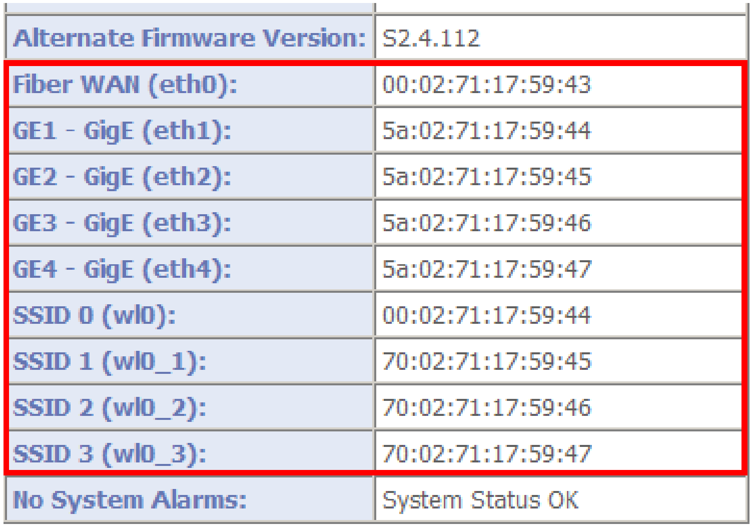
UI Label	Description
System Date and Time	**System Date and Time** is drawn from SNTP (Simple Network Time Protocol) servers. Multiple servers are given in case access to the server is lost. Selecting the SNTP server and other settings can be configure in Internet time, page 37.
System UpTime	**System UpTime** displays the duration of time since the device was last booted. This information can be useful when troubleshooting.
Model Number	The model number of the device. This information is useful when describing the device for troubleshooting. This information is read only and cannot be changed.
Serial Number	Uniquely identifies the device within the context of Model Number & Serial Number.
Registration ID	The identification number entered when the ONU is to be registered using the Reg ID programming procedure (described in the Release Notes).
FSAN	A number that uniquely identifies the device on the PON to the OLT
Bootloader Version	Level of firmware used to load the ONU. This information can be useful when troubleshooting.
Firmware Version	Level of firmware actively running the device. This information can be useful when troubleshooting.
Alternate Firmware Version	Level of firmware residing in the ONU but not currently running.
Interface Names	Each interface has its own unique MAC address. The interface name is shown (Fiber WAN— the network facing interface,GE1, GE2 and so on are subscriber facing interfaces).
System Alarms	This display shows if any alarms are currently active on the system if any. This example shows that no alarms are now present.

Figure 34: Bootloader and firmware version



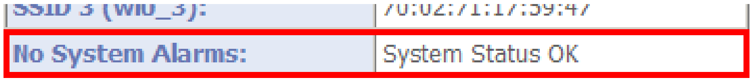
FSAN:	ZNTS03175943
Bootloader Version:	1.0.38-111.42 (2.4.032)
Firmware Version:	S2.4.032
Alternate Firmware Version:	M2.4.025
Fiber WAN (eth0):	00:02:71:17:59:43
GE1 - GigE (eth1):	5a:02:71:17:59:44

Figure 35: MAC addresses are shown for each port



Alternate Firmware Version:	S2.4.112
Fiber WAN (eth0):	00:02:71:17:59:43
GE1 - GigE (eth1):	5a:02:71:17:59:44
GE2 - GigE (eth2):	5a:02:71:17:59:45
GE3 - GigE (eth3):	5a:02:71:17:59:46
GE4 - GigE (eth4):	5a:02:71:17:59:47
SSID 0 (wl0):	00:02:71:17:59:44
SSID 1 (wl0_1):	70:02:71:17:59:45
SSID 2 (wl0_2):	70:02:71:17:59:46
SSID 3 (wl0_3):	70:02:71:17:59:47
No System Alarms:	System Status OK

Figure 36: Alarms example with no alarms presently showing

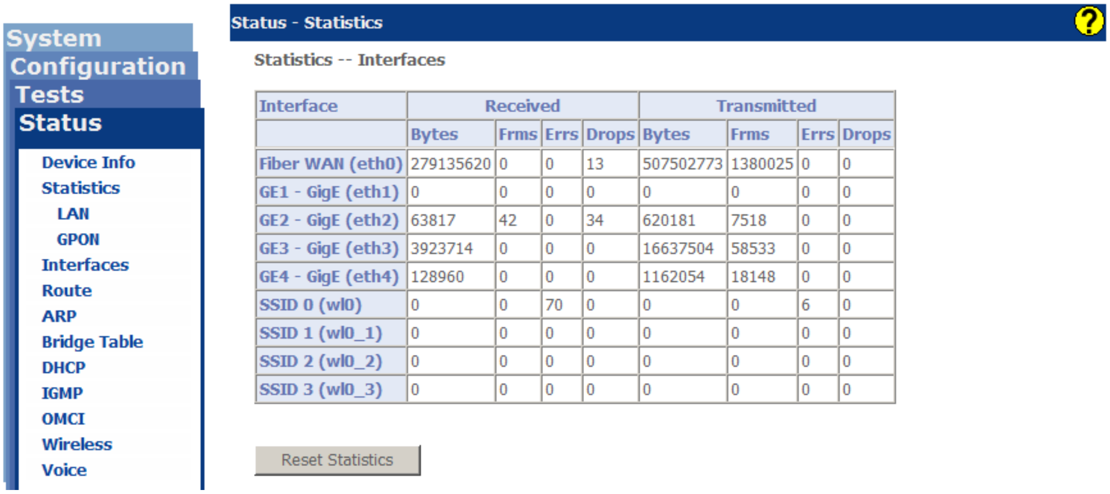


SSID 3 (wl0_3):	70:02:71:17:59:47
No System Alarms:	System Status OK

Statistics

The device maintains counters for the number of bytes and frames that are transmitted as well as received for every Ethernet interface on the ONU, including the Fiber WAN uplink interface (Either GPON or GigE) and the Wireless LAN interface.

Figure 37: LAN side statistics



Status - Statistics

Statistics -- Interfaces

Interface	Received				Transmitted			
	Bytes	Frms	Errs	Drops	Bytes	Frms	Errs	Drops
Fiber WAN (eth0)	279135620	0	0	13	507502773	1380025	0	0
GE1 - GigE (eth1)	0	0	0	0	0	0	0	0
GE2 - GigE (eth2)	63817	42	0	34	620181	7518	0	0
GE3 - GigE (eth3)	3923714	0	0	0	16637504	58533	0	0
GE4 - GigE (eth4)	128960	0	0	0	1162054	18148	0	0
SSID 0 (wl0)	0	0	70	0	0	0	6	0
SSID 1 (wl0_1)	0	0	0	0	0	0	0	0
SSID 2 (wl0_2)	0	0	0	0	0	0	0	0
SSID 3 (wl0_3)	0	0	0	0	0	0	0	0

The LAN side interfaces uses Ethernet statistics and shows the number of received and transmitted bytes, frames, errors and drops.

Resetting the statistics by clicking **Reset Statistics** is a good means of determining if frames are being sent or received, or if errors or drops are still occurring.

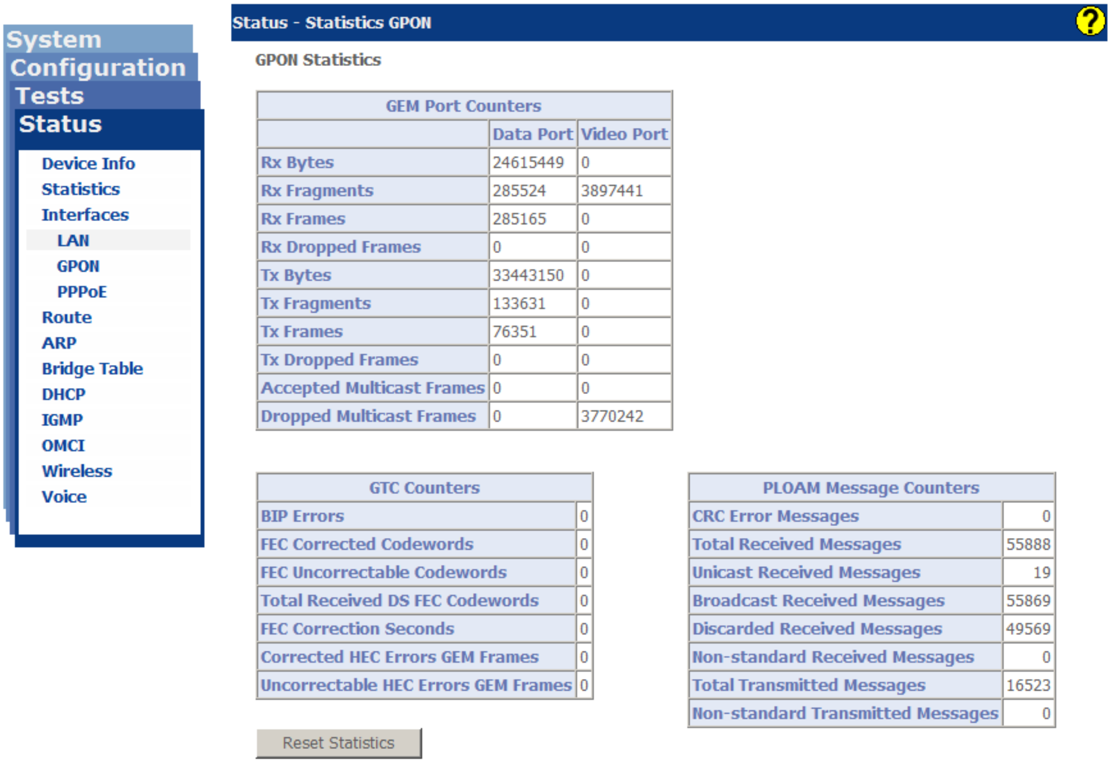
Table 11: LAN side statistics

UI Label	Description
Received Bytes	The number of ingress bytes into the interface, since statistics were last reset. This is the data coming into the ONU from an external source.
Received Frms	The number of ingress frames into the interface, since statistics were last reset. This is the data coming into the ONU from an external source.
Received Errs	The number of ingress frames that were received in error on the interface, since statistics were last reset.
Received Drops	The number of ingress frames that were received in error on the interface, since statistics were last reset due to addressing errors or memory limitations.
Transmitted Bytes	The number of egress bytes transmitted out the interface, since statistics were last reset. This is the data going to an external device.

Table 11: LAN side statistics

UI Label	Description
Transmitted Frms	The number of egress frames transmitted out the interface, since statistics were last reset. This is the data going to an external device.
Transmitted Errs	The number of frames that could not be transmitted from the interface due to framing errors, since statistics were last reset.
Transmitted Drops	The number of egress frames that were dropped (not transmitted) due to addressing errors or memory limitations, since statistics were last reset.

Figure 38: GPON statistics



GPON Statistics

GEM Port Counters		
	Data Port	Video Port
Rx Bytes	24615449	0
Rx Fragments	285524	3897441
Rx Frames	285165	0
Rx Dropped Frames	0	0
Tx Bytes	33443150	0
Tx Fragments	133631	0
Tx Frames	76351	0
Tx Dropped Frames	0	0
Accepted Multicast Frames	0	0
Dropped Multicast Frames	0	3770242

GTC Counters	
BIP Errors	0
FEC Corrected Codewords	0
FEC Uncorrectable Codewords	0
Total Received DS FEC Codewords	0
FEC Correction Seconds	0
Corrected HEC Errors GEM Frames	0
Uncorrectable HEC Errors GEM Frames	0

PLOAM Message Counters	
CRC Error Messages	0
Total Received Messages	55888
Unicast Received Messages	19
Broadcast Received Messages	55869
Discarded Received Messages	49569
Non-standard Received Messages	0
Total Transmitted Messages	16523
Non-standard Transmitted Messages	0

GPON Encapsulation Method (GEM) port is used to transmit frames between the upstream Optical Line Terminal (OLT) and the Optical Network Terminal (ONT), which in this case is the zNID.

Table 12: GPON: GEM port counters

UI Label	Description
Rx Bytes	Number of bytes received on this GEM port, not including GEM headers.
Rx Fragments	Number of GEM fragments received on this GEM port.

Table 12: GPON: GEM port counters

UI Label	Description
Rx Frames	Number of ethernet frames received on this GEM port.
Rx Dropped Frames	Number of receive ethernet frames dropped due to congestion or because frame is undersized.
Tx Bytes	Number of bytes transmitted on this GEM port, not including GEM headers.
Tx Fragments	Number of GEM fragments transmitted on this GEM port.
Tx Frames	Number of ethernet frames transmitted on this GEM port.
Tx Dropped Frames	Number of ethernet frames dropped due to congestion.
Accepted Multicast Frames	Number of multicast frames accepted by the Multicast Filtering Function. IPTV is generally multicast.
Dropped Multicast Frames	Number of multicast frames dropped by the Multicast Filtering Function.

The OLT is the centrally located aggregation point of the optical network and Optical Network Units (ONU) or ONTs are installed at the customer premises. The GPON GTC counters show the error statistics on the optical network to the zNID in question.

Table 13: GPON: GTC (GPON Transmission Convergence Statistics) counter

UI Label	Description
BIP Errors	Bit Interleaved Parity Errors.
FEC Corrected Codewords	Forward Error Coding Corrected Codewords.
FEC UnCorrectable Codewords	Forward Error Coding Uncorrectable Codewords
Total Received DS FEC Codewords	Total Received Downstream Forward Error Coding Codewords.
FEC Correction Seconds	Number of seconds during which there was a FEC correction anomaly.
Corrected HEC errors GEM Frames	Number of GEM frames with corrected HEC errors.
Uncorrected HEC errors GEM Frames	Number of GEM frames with uncorrectable HEC errors.

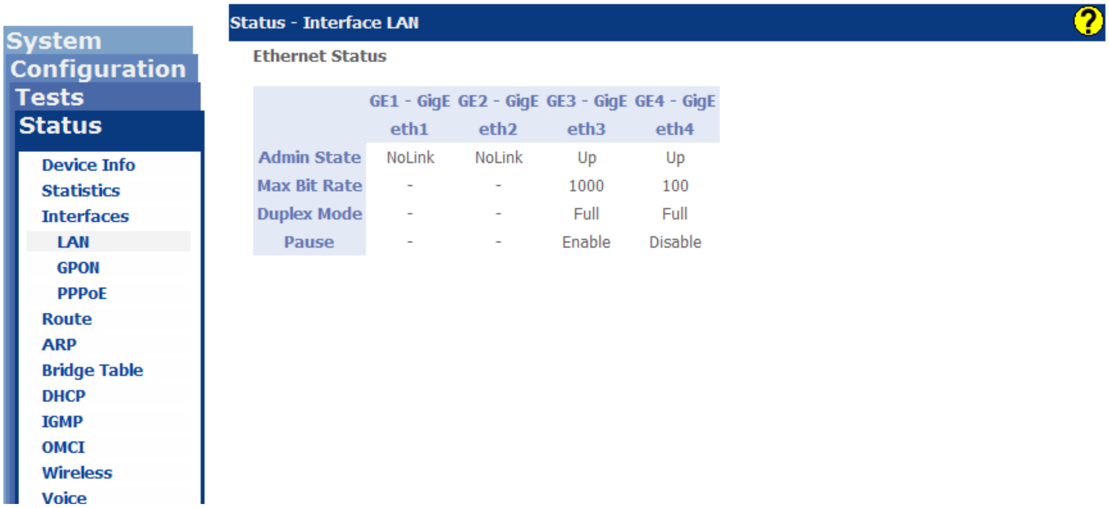
Table 14: PLOAM (Physical Layer Operations and Maintenance) message counters

UI Label	Description
CRC Error Messages	Messages received in error and discarded.
Total Received Messages	Total Number of CRC correct downstream PLOAM messages received.
Unicast Received Messages	Number of CRC correct downstream PLOAM messages with ONU ID matching this ONU's ID.
Broadcast Received Messages	Number of CRC correct broadcast downstream PLOAM messages.
Discarded Received Messages	Number of downstream PLOAM messages discarded, because the message is unknown and not registered, or because the message is not valid in the current state.
Non-standard Received Messages	Number of non-standard downstream PLOAM messages received.
Total Transmitted Messages	Total number of PLOAM messages sent.
Non-standard Transmitted Messages	Number of non-standard downstream PLOAM messages sent.

LAN interface status

The **Status | Interfaces | LAN** screen can be used to see if the interface is up (not only the interface is up, but if it has link with a downstream device).

Figure 39: Status of LAN interfaces



Status - Interface LAN

Ethernet Status

	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4
Admin State	NoLink	NoLink	Up	Up
Max Bit Rate	-	-	1000	100
Duplex Mode	-	-	Full	Full
Pause	-	-	Enable	Disable

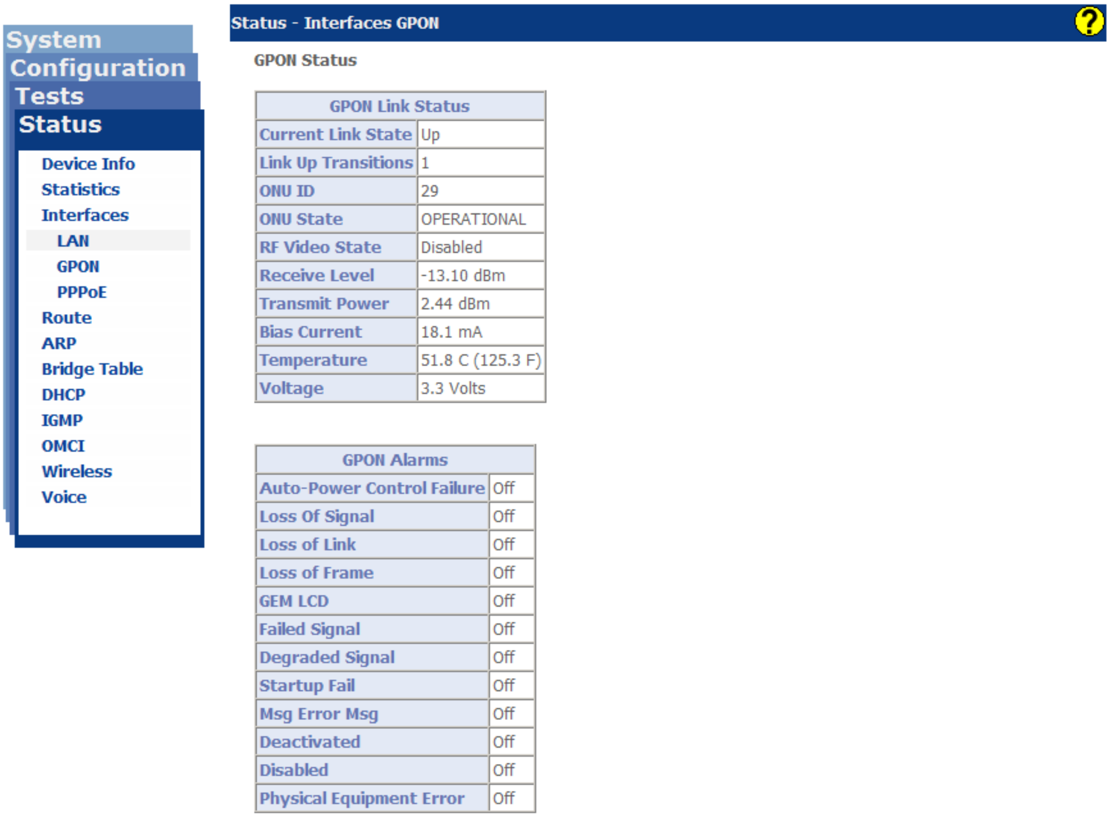
Table 15: LAN interface Ethernet status

UI Label	Description
Admin State	• **Up** Port is enabled and a link has been established. • **Down** Port is disabled (administratively down). • **NoLink** Ethernet Port is enabled, but no device is connected
Max Bit Rate	Shows the bit rate of the physical layer: • **10** — 10 Mbps • **100** — 100 Mbps • **1000** — 1 Gbps
Duplex Mode	Full or Half Duplex
Pause	• **Enable** Port will transmit pause frames to an attached device when there is receive congestion. • **Disable** Port will not transmit pause frames to an attached device

GPON interface status

The **Status | Interfaces | GPON** screen can be used to see if the interface is up, the ONU ID, and other information and alarms.

Figure 40: Status of GPON interfaces



GPON Status

GPON Link Status	
Current Link State	Up
Link Up Transitions	1
ONU ID	29
ONU State	OPERATIONAL
RF Video State	Disabled
Receive Level	-13.10 dBm
Transmit Power	2.44 dBm
Bias Current	18.1 mA
Temperature	51.8 C (125.3 F)
Voltage	3.3 Volts

GPON Alarms	
Auto-Power Control Failure	Off
Loss Of Signal	Off
Loss of Link	Off
Loss of Frame	Off
GEM LCD	Off
Failed Signal	Off
Degraded Signal	Off
Startup Fail	Off
Msg Error Msg	Off
Deactivated	Off
Disabled	Off
Physical Equipment Error	Off

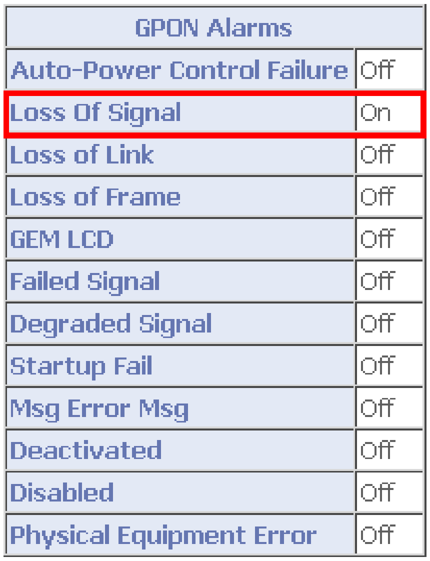
Table 16: GPON link status

UI Label	Description
Current Link State	• Up — link is active. • Down — link is not communicating
Link Up Transitions	Number of times the Link has transitioned from down to up.
ONU ID	Optical Network Unit ID.
ONU State	Optical Network Unit State. OPERATIONAL is active.
RF Video State	Indicates interface is enabled or disabled.
Receive Level	The optical receive level, in dBm.
Transmit Power	The optical transmit level, in dBm.
Bias Current	Transmitting laser bias current, in mA.

Table 16: GPON link status

UI Label	Description
Triplexer Temp	Temperature of the triplexer device, in degrees C (and F).
Voltage	Nominal triplexer operating voltage.

Figure 41: GPON alarm example, Loss of Signal



GPON Alarms	
Auto-Power Control Failure	Off
Loss Of Signal	On
Loss of Link	Off
Loss of Frame	Off
GEM LCD	Off
Failed Signal	Off
Degraded Signal	Off
Startup Fail	Off
Msg Error Msg	Off
Deactivated	Off
Disabled	Off
Physical Equipment Error	Off

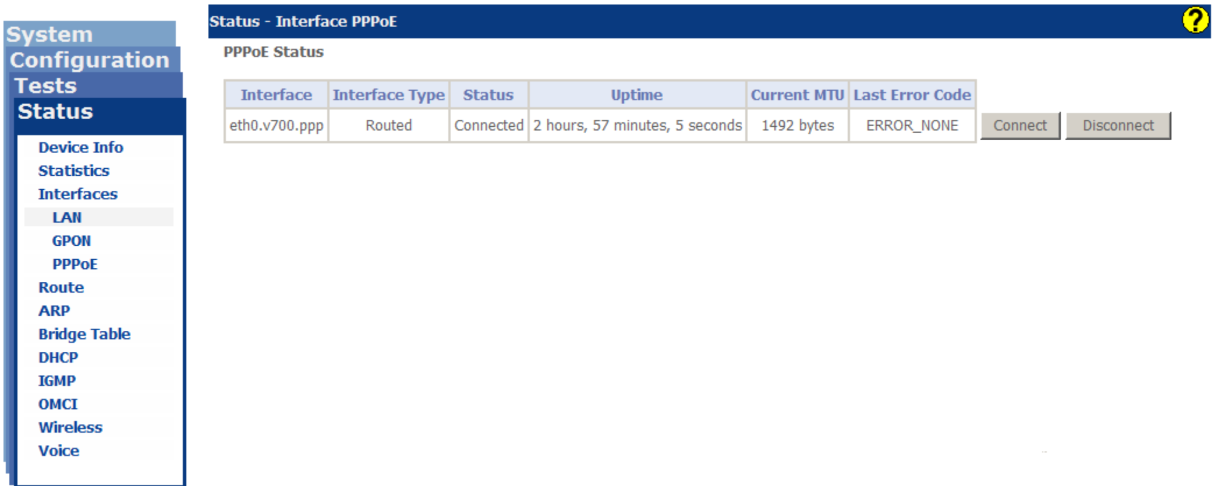
Table 17: GPON alarms

UI Label	Description
Auto-Power Control Failure	Auto-Power Control (APC) is the ability to adjust to variations in optical power. APC failure is the inability to properly adjust.
Loss of Signal	No input signal detected. Make sure fiber is plugged in.
Loss of Link	The link has been lost
Loss of Frame	Framing has been lost
GEM LCD	Loss of GEM Channel Delineation.
Failed Signal	Bit Error Rate exceeds 10E-5
Degraded Signal	Bit Error Rate exceeds 10E-6
Msg Error Msg	Unknown PLOAM message received.
Deactivated	Received Deactivate on ONU.
Disabled	Disabled by the OLT or the ONU Serial Number is not configured on the OLT.
Physical Equipment Error	Indicates possible hardware problems.

PPPoE status

This table provides interface status for each PPPoE uplink tunnel. This status includes the time that the connection has been up the configured MTU size, and the last error code reported for this interface.

Figure 42: PPPoE status



Status - Interface PPPoE

PPPoE Status

Interface	Interface Type	Status	Uptime	Current MTU	Last Error Code
eth0.v700.ppp	Routed	Connected	2 hours, 57 minutes, 5 seconds	1492 bytes	ERROR_NONE

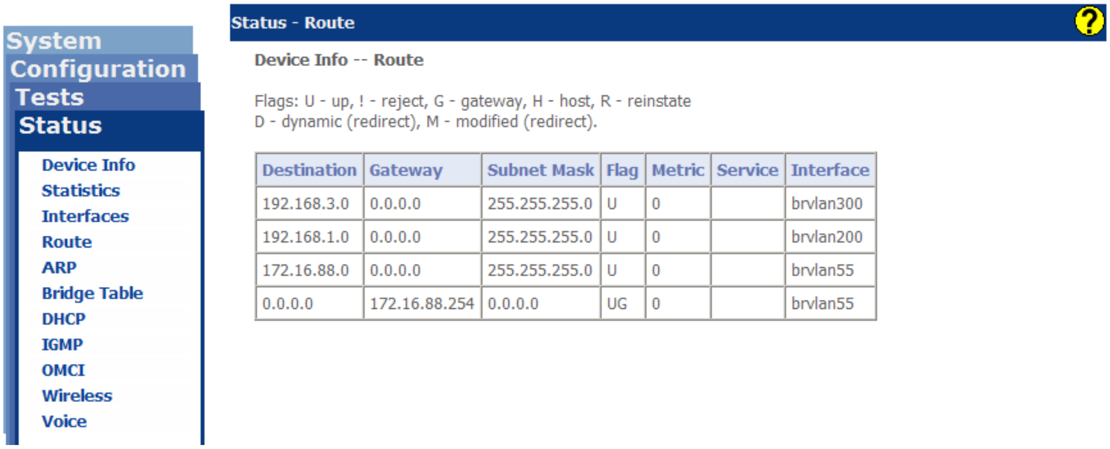
Table 18: PPPoE status

UI Label	Description
Interfaces	Name of the PPP Uplink Interface.
Interface Type	Bridged or Routed.
Status	Current status of the PPP protocol.
Uptime	Duration that the PPP protocol has been connected.
Current MTU	The current Maximum Transmission Unit size.
Last Error Code	Last Error encountered.
Connect Button	Connect or reconnect.
Disconnect Button	Disconnect and leave disconnected.

Route

The **Route** page shows the essential elements of the zNID’s routing table.

Figure 43: Route table



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
192.168.3.0	0.0.0.0	255.255.255.0	U	0		brvlan300
192.168.1.0	0.0.0.0	255.255.255.0	U	0		brvlan200
172.16.88.0	0.0.0.0	255.255.255.0	U	0		brvlan55
0.0.0.0	172.16.88.254	0.0.0.0	UG	0		brvlan55

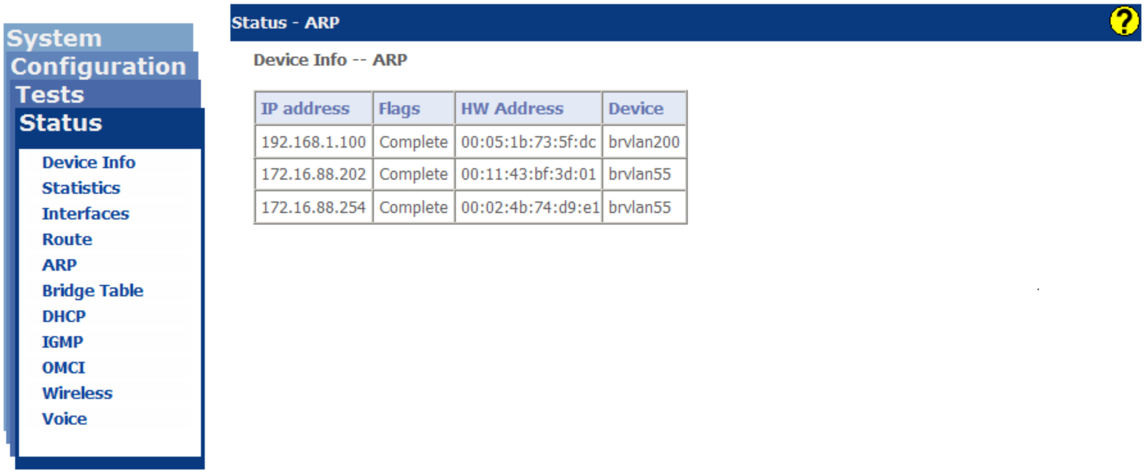
Table 19: The route table

UI Label	Description
Destination	IP address or range of addresses for the static IP address (or range of addresses) in the routing table.
Gateway	IP Address of Next Hop Router
Subnet Mask	The subnet mask determines the network portion of the address. The 255 in an octet masks all information from that octet.
Flag	• **U** - Route is up and available for use • **!** - Rejecting route - all packets to this network are dropped • **G** - Specified Gateway should be used for this route. • **H** - Host • **R** - Reinstate • **D** - Dynamically installed route table entry • **M** - Modified route table entry (typically by ICMP redirect).
Metric	Defines the “Number of Hops” to reach the destination. The metric value is used to determine which route to use, Routes with lower metrics are chosen first.
Service	IP Service Connection interface name
Interface	The bridge interface for which the route is defined.

ARP table

This table displays the IP and MAC address for each device on a VLAN.

Figure 44: ARP table



Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.100	Complete	00:05:1b:73:5f:dc	brvlan200
172.16.88.202	Complete	00:11:43:bf:3d:01	brvlan55
172.16.88.254	Complete	00:02:4b:74:d9:e1	brvlan55

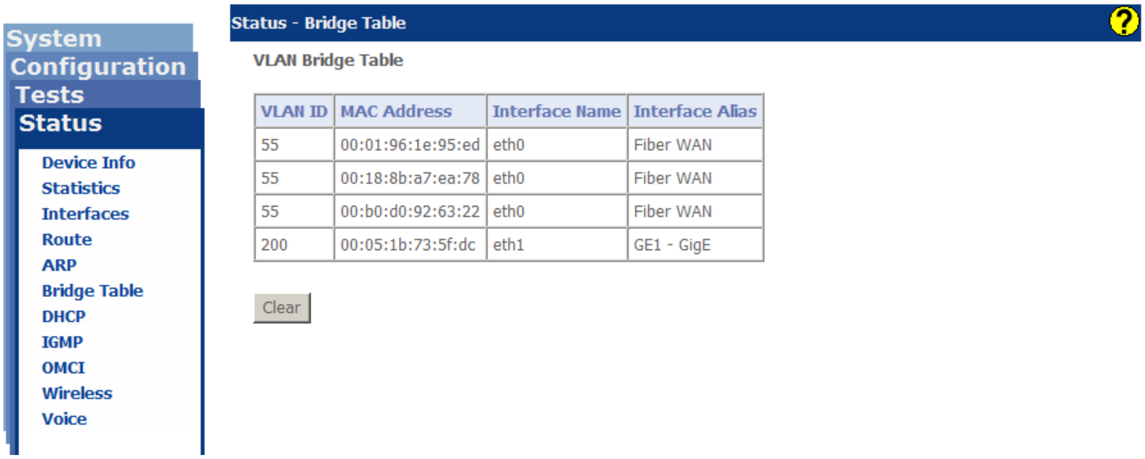
Table 20: The ARP table

UI Label	Description
IP Address	The IP address of the device discovered on the interface listed in the device column.
Flags	• **Complete** – Both IP and MAC address have been resolved • **Permanent** – Statically configured ARP entry • **Publish** – Proxy ARP entry • **Incomplete** – IP or MAC but not both
HW Address	MAC address of the device discovered on the interface listed in the device column.
Device	The Bridge interface or logical VLAN interface of the internal layer 2 bridge on which the device was discovered.

Bridge table

The bridge table displays the MAC address for each device on a VLAN interface of the internal layer 2 bridge. A total of 4,096 entries are allowed in the bridge table, but only the 2048 most recent entries are displayed. The bridge table can give you an idea of the number of devices that are seen on the network.

Figure 45: Bridge table



VLAN Bridge Table

VLAN ID	MAC Address	Interface Name	Interface Alias
55	00:01:96:1e:95:ed	eth0	Fiber WAN
55	00:18:8b:a7:ea:78	eth0	Fiber WAN
55	00:b0:d0:92:63:22	eth0	Fiber WAN
200	00:05:1b:73:5f:dc	eth1	GE1 - GigE

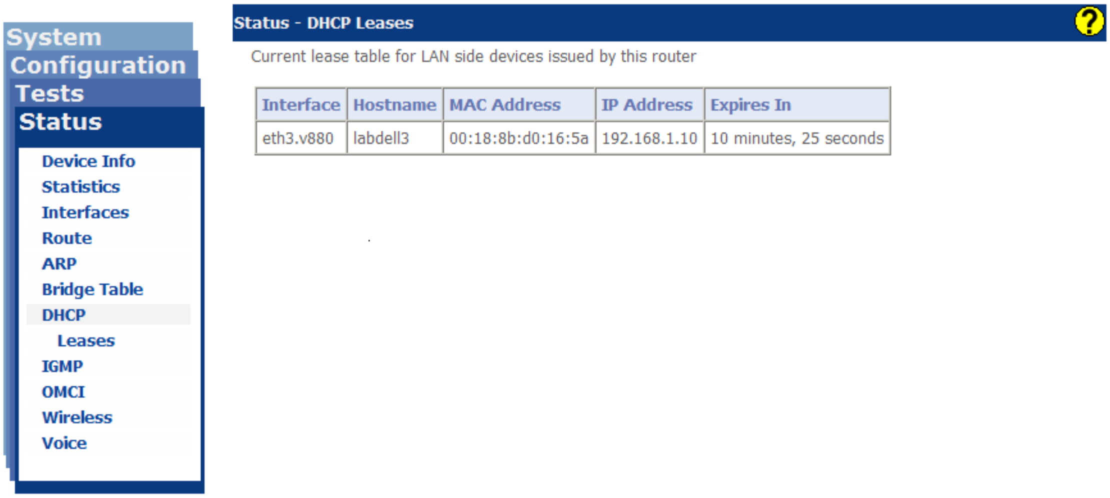
Table 21: The VLAN Bridge table

UI Label	Description
VLAN ID	The Bridge interface or logical VLAN interface of the internal layer 2 bridge on which the device was discovered
MAC Address	MAC address of the discovered device
Interface Name	The Linux Interface Name for the port on which the MAC address was discovered
Interface Alias	The name created for the interface to help the user match the port to the Linux Interface Name

DHCP status

DHCP status provides a table of DHCP leases given out by the ONU's internal DHCP Server.

Figure 46: DHCP server device information and status



Status - DHCP Leases

Current lease table for LAN side devices issued by this router

Interface	Hostname	MAC Address	IP Address	Expires In
eth3.v880	labdell3	00:18:8b:d0:16:5a	192.168.1.10	10 minutes, 25 seconds

This page shows the computers, identified by the hostname and MAC address that have acquired IP addresses by the DHCP server with the time remaining before the lease for the IP address is up.

If conditional DHCP server is configured, there is a page (Status|DHCP|Bindings which shows the permanently assigned IP address.

Table 22: Table of DHCP Leases given out by the internal DHCP Server

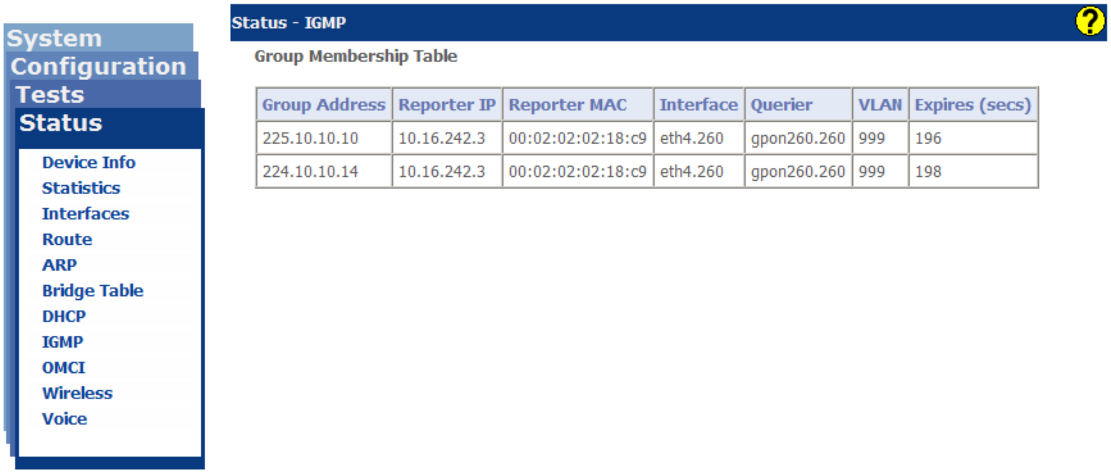
UI Label	Description
Interface	Name of the interface or virtual interface that received a request for an IP address from the internal DHCP server.
Host Name	Name of the device that requested an IP address from the internal DHCP Server.
MAC Address	The MAC address of the device that requested an IP Address.
IP Address	The IP address that assigned to the device by the DHCP server.
Expires In	The time remaining before the lease for this IP address runs out.

IGMP

Internet Group Management Protocol (IGMP) is used to create group memberships for multicast streams. Normally IGMP is used for streaming video and other applications such as gaming, to provide more efficient use of the networks resources for these types of applications.

See *Creating video connections* on page 190 for configuration information.

Figure 47: The group membership table for IGMP



Status - IGMP

Group Membership Table

Group Address	Reporter IP	Reporter MAC	Interface	Querier	VLAN	Expires (secs)
225.10.10.10	10.16.242.3	00:02:02:02:18:c9	eth4.260	gpon260.260	999	196
224.10.10.14	10.16.242.3	00:02:02:02:18:c9	eth4.260	gpon260.260	999	198

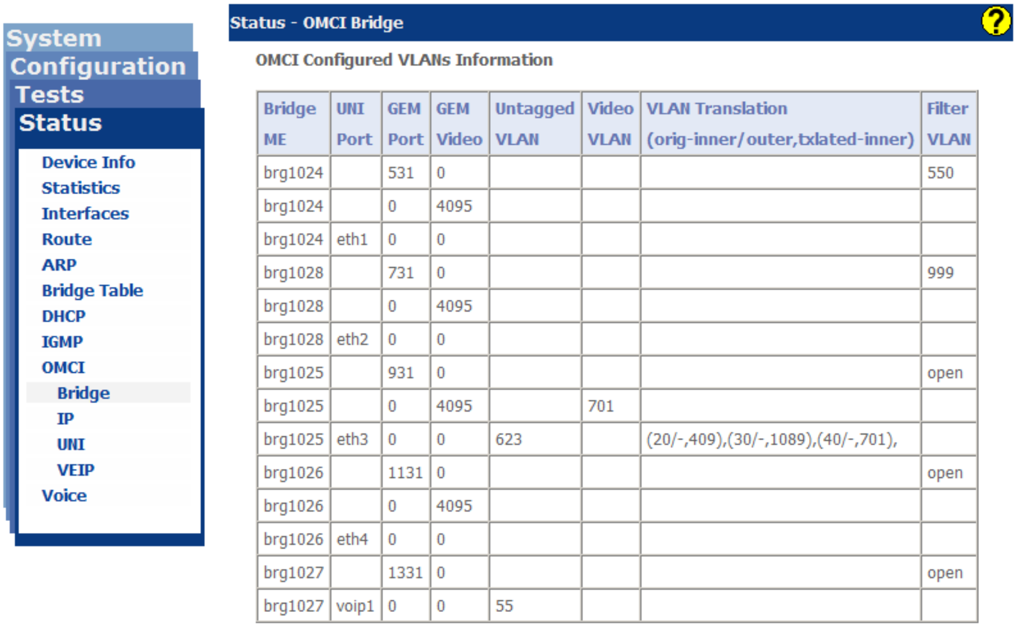
Table 23: Table of IGMP group members

UI Label	Description
Group Address	Multicast IP group address.
Reporter IP	The IP address of the host in the multicast group.
Reporter MAC	The MAC address of the host in the multicast group.
Interface	The Interface which discovered the multicast group.
VLAN	The VLAN which discovered the multicast group.
Querier	TBD
Expires	The time before the multicast group is timed out.

OMCI

The OMCI bridge table displays the GPON Bridges that are mapped to GEM ports with VLAN Filter and translation rules. These are the “Pure ONU” traffic flows that have been configured via OMCI commands from the OLT. This information is useful for debug of OMCI-related configuration issues.

Figure 48: OMCI bridge



OMCI Configured VLANs Information

Bridge ME	UNI Port	GEM Port	GEM Video	Untagged VLAN	Video VLAN	VLAN Translation (orig-inner/outer,txlated-inner)	Filter VLAN
brg1024		531	0				550
brg1024		0	4095				
brg1024	eth1	0	0				
brg1028		731	0				999
brg1028		0	4095				
brg1028	eth2	0	0				
brg1025		931	0				open
brg1025		0	4095		701		
brg1025	eth3	0	0	623		(20/-,409),(30/-,1089),(40/-,701),	
brg1026		1131	0				open
brg1026		0	4095				
brg1026	eth4	0	0				
brg1027		1331	0				open
brg1027	voip1	0	0	55			

Table 24: OMCI mapping information for bridged interface

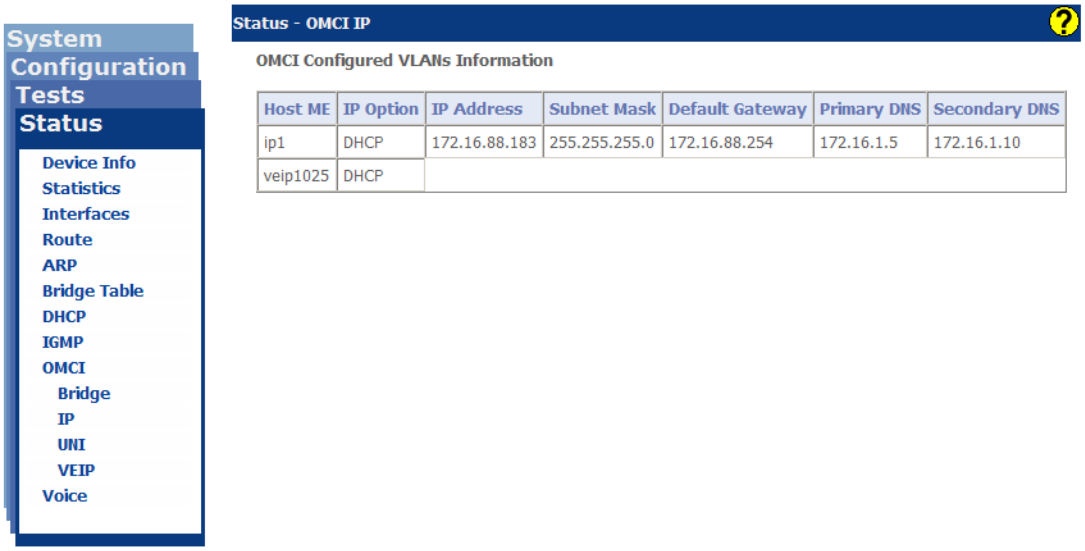
UI Label	Description
Bridge ME	The ID number assigned by the OLT for this instance of an OMCI-configured GPON Bridge.
UNI Port	The UNI port (Ethernet, VOIP, VEIP) that is associated with this Bridge ME.
GEM Port	The GEM port on the GPON link that is associated with this Bridge ME.
GEM Video	(Optional) The Multicast GEM port on the GPON link that is associated with this Bridge ME.
Untagged VLAN	The default tag that will be applied on ingress for untagged packets. In the egress direction, this tag will be stripped.
Video VLAN	(Optional) The VLAN ID for multicast video traffic sent/received using Bridge ME.
VLAN Translation	(Optional) The VLAN translation actions that are configured for this Bridge ME.

Table 24: OMCI mapping information for bridged interface

UI Label	Description
Filter VLAN	The VLAN IDs of downstream traffic that will be allowed to pass through the unit. All packets with VLAN IDs that do not match will be dropped. When configured for “OPEN” mode, all VLAN IDs are allowed to pass through.

The OMCI IP table displays the IP Host instances that have been configured by the OLT using OMCI commands. This information is useful for debug of OMCI-related configuration issues.

Figure 49: OMCI mapping information for bridged interface



Status - OMCI IP

OMCI Configured VLANs Information

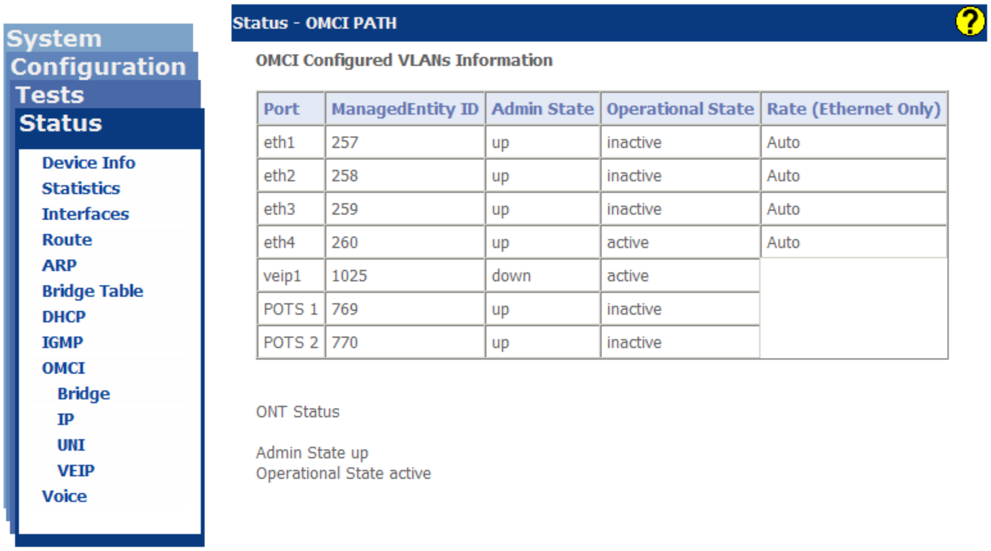
Host ME	IP Option	IP Address	Subnet Mask	Default Gateway	Primary DNS	Secondary DNS
ip1	DHCP	172.16.88.183	255.255.255.0	172.16.88.254	172.16.1.5	172.16.1.10
veip1025	DHCP					

Table 25: OMCI mapping information for routed interface

UI Label	Description
Host ME	The instance of the OMCI-configured IP Host.
IP Option	The IP Address Mode for this IP Host instance. Choices are Static and DHCP.
IP Address	The IP Address assigned to this IP Host or acquired via DHCP.
Subnet Mask	The Subnet Mask to be used by this IP Host instance.
Default Gateway	The Default Gateway to be used by this IP Host instance.
Primary DNS	The Primary DNS to be used by this IP Host instance.
Secondary DNS	The Secondary DNS to be used by this IP Host instance.

The OMCI Path table displays the Managed Entity IDs that have been assigned by the OLT to each of the Physical and Virtual User-to-Network Interfaces (UNIs), along with their Administrative and Operational State. OMCI commands can Admin Down any of these interfaces. When Admined Down, they are unusable for any services. This information is useful for debug of OMCI-related configuration issues.

Figure 50: OMCI mapping information for VLANS



Status - OMCI PATH

OMCI Configured VLANs Information

Port	ManagedEntity ID	Admin State	Operational State	Rate (Ethernet Only)
eth1	257	up	inactive	Auto
eth2	258	up	inactive	Auto
eth3	259	up	inactive	Auto
eth4	260	up	active	Auto
veip1	1025	down	active	
POTS 1	769	up	inactive	
POTS 2	770	up	inactive	

ONT Status

Admin State up
Operational State active

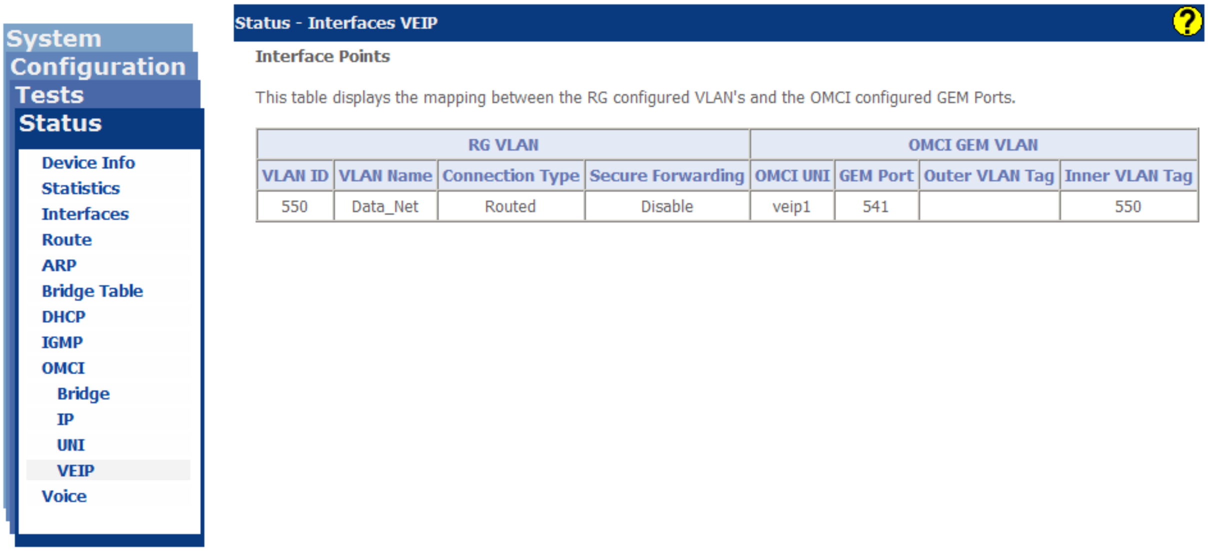
Table 26: OMCI mapping information for VLANS

UI Label	Description
Port	The Physical and Virtual User-to-Network Interfaces that are configurable via OMCI.
ManagedEntity ID	The OMCI instance of the UNI.
Admin State	When configured **Down**, the port is unusable. Must be configured **Up** for normal operation. This is controlled by the OLT via OMCI commands.
Operational State	The Operational Status of the UNI as reported by the device to the OLT.
Rate (Ethernet Only)	The OMCI-configured Port Rate and Duplex Mode.

The Interfaces VEIP table displays the configured VLAN that are mapped to an uplink GEM Port. The uplink GEM port is required to be configured via OMCI. This table display the final mapping of the user defined RG VLANs and the OMCI configured GEM ports and VLANs.

The OMCI mapping to the RG VLAN occurs when the OMCI dynamic provisioning feature of the MXK is used to provision the OMCI-side of the VEIP and it uses SNMP to create the RG side of the VEIP.

Figure 51: OMCI mapping information for VEIP mapping



Status - Interfaces VEIP

Interface Points

This table displays the mapping between the RG configured VLAN's and the OMCI configured GEM Ports.

RG VLAN				OMCI GEM VLAN			
VLAN ID	VLAN Name	Connection Type	Secure Forwarding	OMCI UNI	GEM Port	Outer VLAN Tag	Inner VLAN Tag
550	Data_Net	Routed	Disable	veip1	541		550

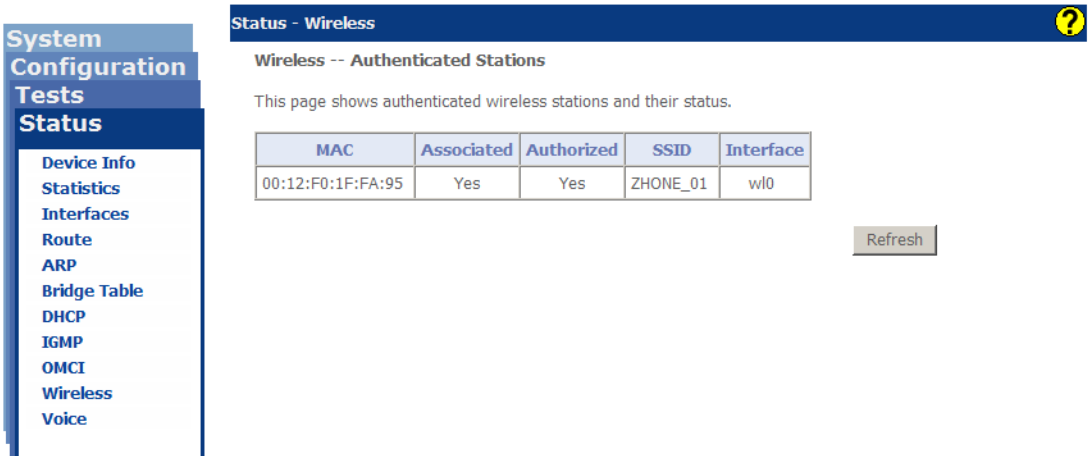
Table 27: Table of IGMP group members

UI Label	Description
VLAN ID	The VLAN Tag for this flow.
VLAN Name	The VLAN Name as defined by the user for this VLAN ID.
Connection Type	Bridged, Routed, PPPoE Bridged, PPPoE Routed and Bridged CPU are types of VLAN connections.
Secure Forwarding	Enabled will result in broadcast frames being discarded.
OMCI UNI	Virtual Ethernet Interface Point.
GEM Port	GPON Encapsulation Method Port. Each GEM port bears one kind of service traffic.
Outer VLAN Tag	The outer VLAN tag for this flow.
Inner VLAN Tab	The inner VLAN tag for this flow.

Wireless

The **Status | Wireless** pages shows the authenticated wireless stations which are access the wireless access point.

Figure 52: Authenticated wireless stations



Status - Wireless

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
00:12:F0:1F:FA:95	Yes	Yes	ZHONE_01	wl0

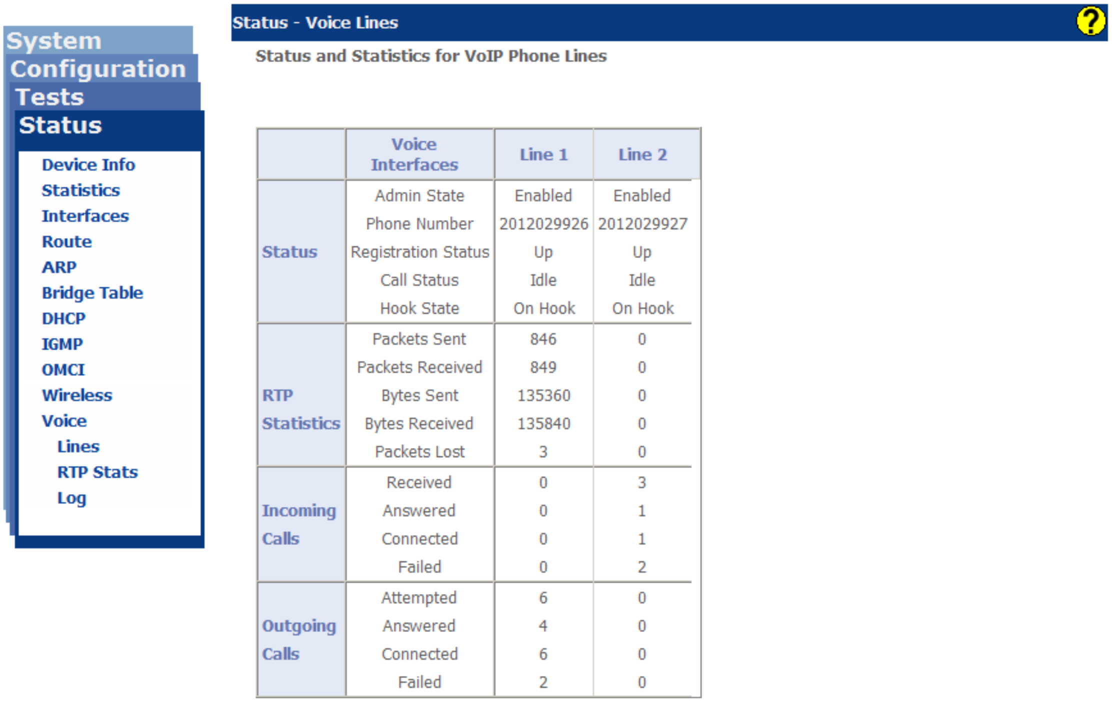
Table 28: Authenticated wireless stations

UI Label	Description
MAC	The MAC address of the authenticated wireless station.
Associated	The wireless station has been associated with the access point.
Authorized	The wireless station is an authorized user of the access point. (The wireless station has successfully completed the authentication process.).
SSID	The SSID of the of the zNID’s access point.
Interface	The interface of the of the zNID’s access point.

Voice

Two types of voice logs are provided by the zNID. Voice Packet Log(s) and Call Audit log(s). The voice packet logs show signalling packets sent to and received from the VoIP softswitch and can be used to debug registration or connectivity issues. The Audit logs show completed incoming and outgoing calls, with date, time, duration of call and phone number and can be used to see calling activity and confirm normal operation.

Figure 53: Status and statistics for voice lines



Status - Voice Lines

Status and Statistics for VoIP Phone Lines

	Voice Interfaces	Line 1	Line 2
Status	Admin State	Enabled	Enabled
	Phone Number	2012029926	2012029927
	Registration Status	Up	Up
	Call Status	Idle	Idle
	Hook State	On Hook	On Hook
RTP Statistics	Packets Sent	846	0
	Packets Received	849	0
	Bytes Sent	135360	0
	Bytes Received	135840	0
	Packets Lost	3	0
Incoming Calls	Received	0	3
	Answered	0	1
	Connected	0	1
	Failed	0	2
Outgoing Calls	Attempted	6	0
	Answered	4	0
	Connected	6	0
	Failed	2	0

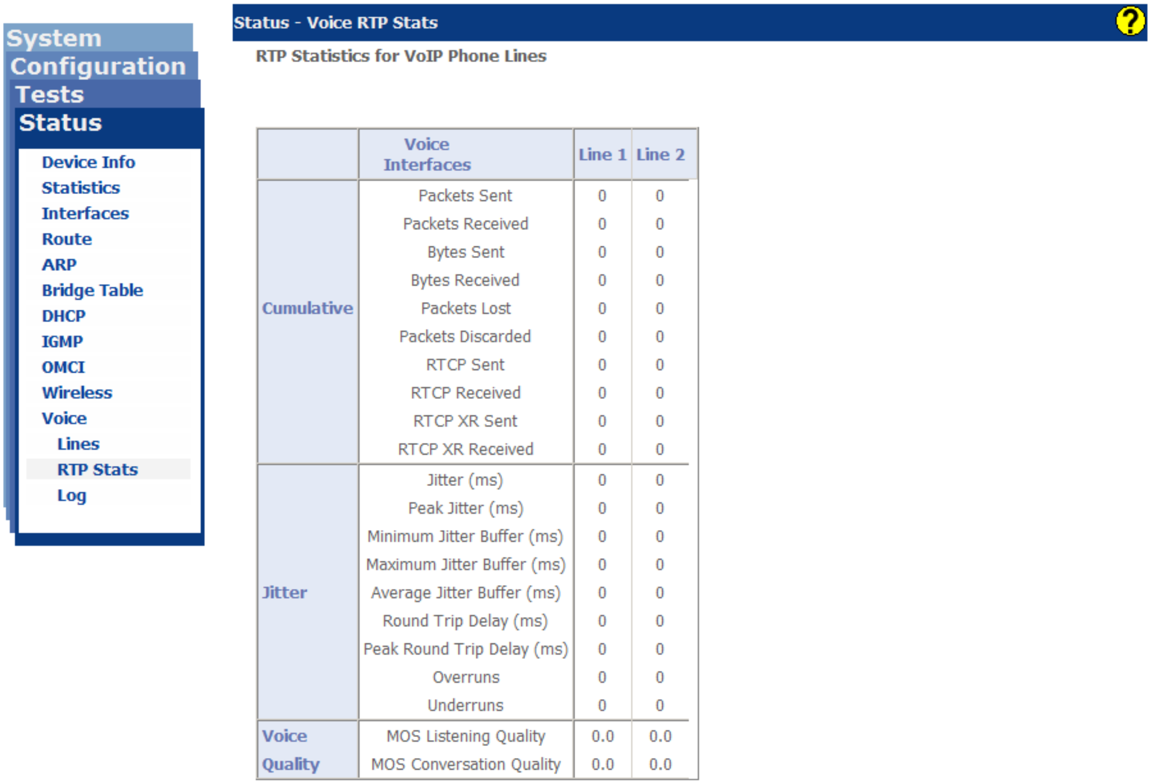
Table 29: Table of VoIP lines status and statistics

UI Label	Description
Status	• **Admin State** – Configured State • **Phone Number** – Configured Phone Number in SIP mode • **Registration Status** – Current Registration status with the Switch • **Call Status** – Current Call Status Idle is no call, InCall means that this side is fully connected • **Hook State** – Shows whether the line is On-hook or Off-hook.

Table 29: Table of VoIP lines status and statistics

UI Label	Description
RTP Statistics	The statistics provided refer to the previous completed call • **Packets Sent** – The number of packetized data buffers sent into the network. • **Packets Received** – The number of packetized data buffer received from the network. • **Bytes Sent** – The cumulative count of data bytes in the packets sent to the network. • **Bytes Received** – The cumulative count of data bytes in the packets received from the network. • **Packets Lost** – Number of packets not received based on sequence numbers.
Incoming Calls	The statistics provided refer to the previous completed call • **Received** – A connect command was received from the Switch and the call is in Receive Only mode so that the phone can ring. • **Answered** – A connect command was received from the Switch and the call is in Send and Receive mode. • **Connected** – A Disconnect that had one or more Packets Received. • **Failed** – A Disconnect that had no Packets Received.
Outgoing Calls	• **Attempted** – Dialed number sent to the switch. • **Answered** – A connect command was received from the Switch and the call is inSend and Receive mode. • **Connected** – A Disconnect that had one or more Packets Received. • **Failed** – A Disconnect that had no Packets Received

Figure 54: Voice Real-Time Packet Protocol statistics



Status - Voice RTP Stats

RTP Statistics for VoIP Phone Lines

	Voice Interfaces	Line 1	Line 2
Cumulative	Packets Sent	0	0
	Packets Received	0	0
	Bytes Sent	0	0
	Bytes Received	0	0
	Packets Lost	0	0
	Packets Discarded	0	0
	RTCP Sent	0	0
	RTCP Received	0	0
	RTCP XR Sent	0	0
	RTCP XR Received	0	0
Jitter	Jitter (ms)	0	0
	Peak Jitter (ms)	0	0
	Minimum Jitter Buffer (ms)	0	0
	Maximum Jitter Buffer (ms)	0	0
	Average Jitter Buffer (ms)	0	0
	Round Trip Delay (ms)	0	0
	Peak Round Trip Delay (ms)	0	0
	Overruns	0	0
	Underruns	0	0
Voice Quality	MOS Listening Quality	0.0	0.0
	MOS Conversation Quality	0.0	0.0

Real-Time Packet Protocol (RTP) statistics can be used to determine activity sent into the network or received from the network on the VoIP lines. RTP is used with Real-time Control Protocol (RTCP) which monitors transmission statistics through control packets sent into or received from the network.

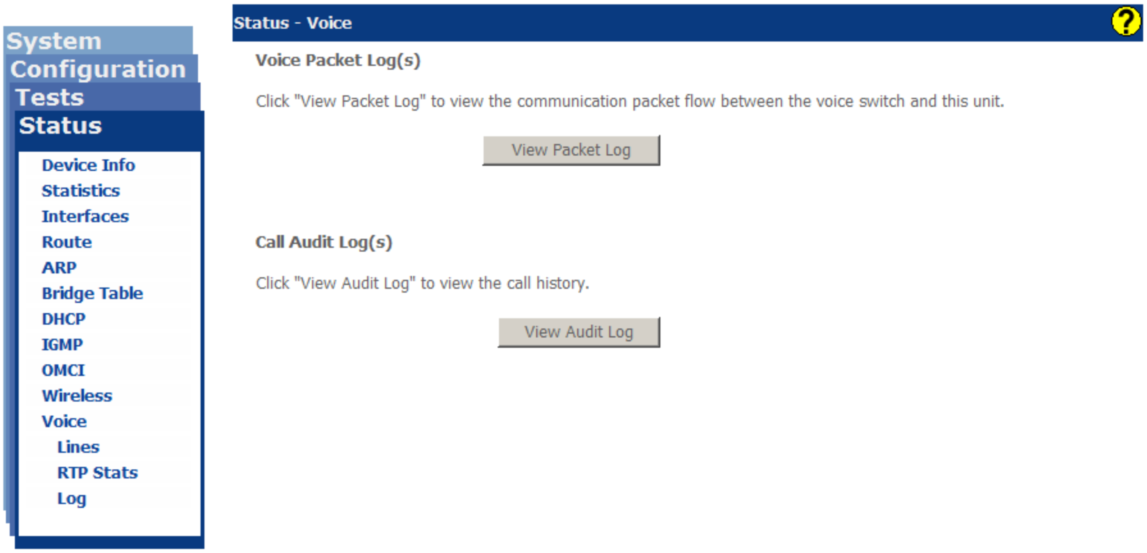
Table 30: RTP statistics

UI Label	Description
Cumulative	Cumulative statistics are kept across call
Packets Sent	The cumulative count of data bytes in the packets sent to the network
Bytes Sent	The cumulative count of data bytes in the packets sent to the network
Bytes Received	The cumulative count of data bytes in the packets received from the network
Packets Lost	The number of packets not received based upon sequence numbers
Packets Discarded	The number of packets received but discarded
RTCP Sent	The number of control packets sent into the network
RTCP Received	The number of control packets received from the network

Table 30: RTP statistics

UI Label	Description
RTCP XR Sent	The number of extended reporting control packets sent into the network (should be the same as RTCP Sent)
RTCP XR Received	The number of extended reporting control packets received from the network
Jitter	Jitter statistics are kept from the previous call
Peak Jitter (ms)	The average delay variation (Jitter) between RTP packets
Minimum Jitter Buffer (ms)	The least delay an RTP packet had passing through the Jitter buffer
Maximum Jitter Buffer (ms)	The greatest delay an RTP packet had passing through the Jitter buffer
Average Jitter Buffer (ms)	The average delay an RTP packet had passing through the Jitter buffer
Round Trip Delay (ms)	The two way network delay
Peak Round Trip Delay (ms)	The worst two way network delay
Overruns	Number of packets received that could not be sent to the Jitter buffer since it was full
Underruns	The number of times the Jitter buffer was empty
Voice Quality	Voice Quality statistics are kept from the previous call
MOS Listening Quality	Mean Opinion Score. On a scale from 0 (poor) to 5 (good)
MOS Conversation Quality	Mean Opinion Score. On a scale from 0 (poor) to 5 (good)

Figure 55: Voice status logs



Status - Voice

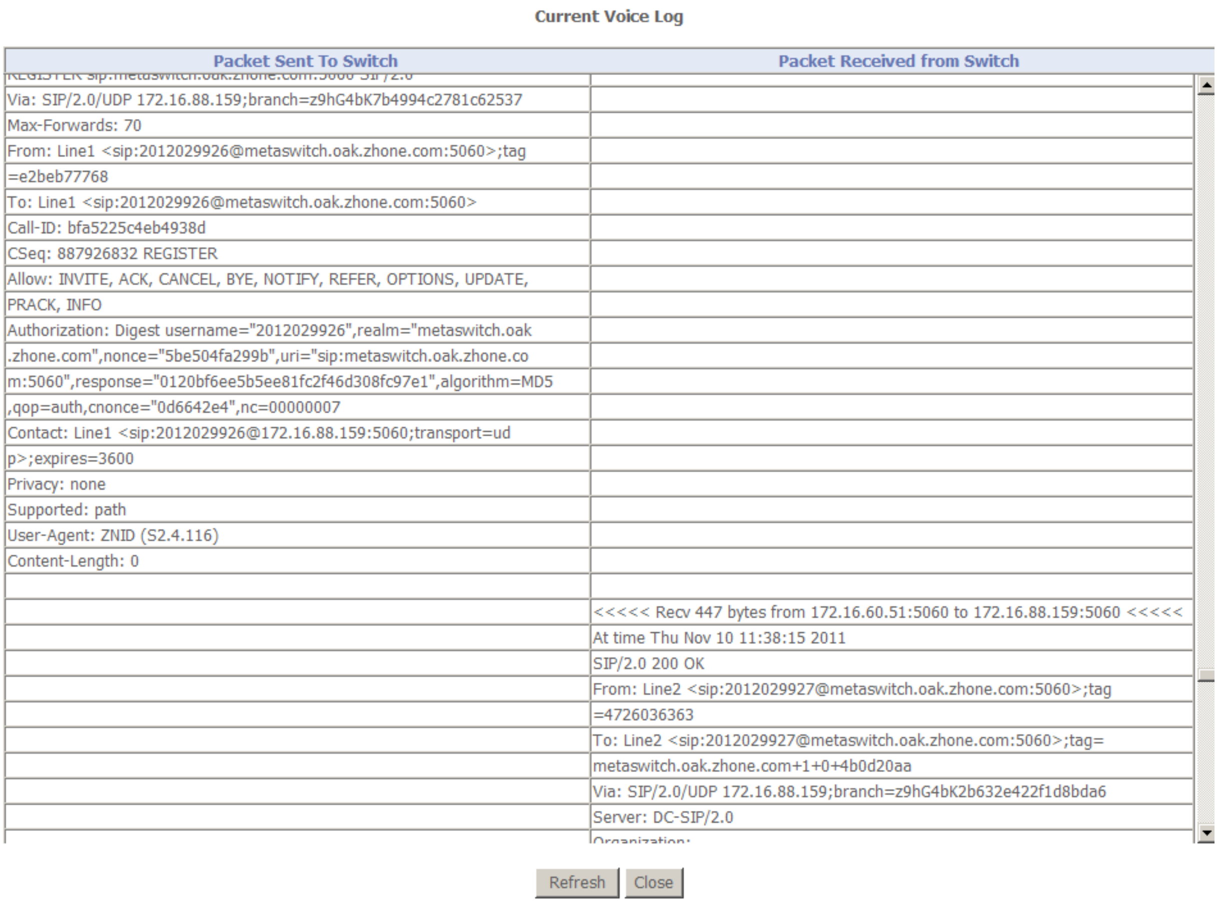
Voice Packet Log(s)

Click "View Packet Log" to view the communication packet flow between the voice switch and this unit.

Call Audit Log(s)

Click "View Audit Log" to view the call history.

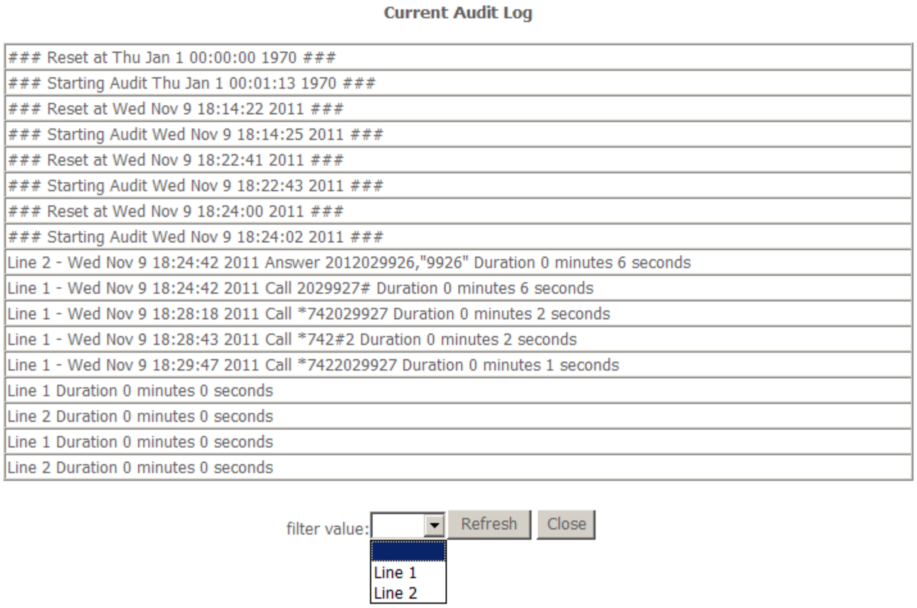
Figure 56: View packet log



Current Voice Log

Packet Sent To Switch	Packet Received from Switch
REGISTER sip:metaswitch.oak.zhone.com:5060 SIP/2.0	
Via: SIP/2.0/UDP 172.16.88.159;branch=z9hG4bK7b4994c2781c62537	
Max-Forwards: 70	
From: Line1 <sip:2012029926@metaswitch.oak.zhone.com:5060>;tag	
=e2beb77768	
To: Line1 <sip:2012029926@metaswitch.oak.zhone.com:5060>	
Call-ID: bfa5225c4eb4938d	
CSeq: 887926832 REGISTER	
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, OPTIONS, UPDATE,	
PRACK, INFO	
Authorization: Digest username="2012029926",realm="metaswitch.oak	
.zhone.com",nonce="5be504fa299b",uri="sip:metaswitch.oak.zhone.co	
m:5060",response="0120bf6ee5b5ee81fc2f46d308fc97e1",algorithm=MD5	
,qop=auth,cnonce="0d6642e4",nc=00000007	
Contact: Line1 <sip:2012029926@172.16.88.159:5060;transport=ud	
p>;expires=3600	
Privacy: none	
Supported: path	
User-Agent: ZNID (S2.4.116)	
Content-Length: 0	
	<<<<< Recv 447 bytes from 172.16.60.51:5060 to 172.16.88.159:5060 <<<<<
	At time Thu Nov 10 11:38:15 2011
	SIP/2.0 200 OK
	From: Line2 <sip:2012029927@metaswitch.oak.zhone.com:5060>;tag
	=4726036363
	To: Line2 <sip:2012029927@metaswitch.oak.zhone.com:5060>;tag=
	metaswitch.oak.zhone.com+1+0+4b0d20aa
	Via: SIP/2.0/UDP 172.16.88.159;branch=z9hG4bK2b632e422f1d8bda6
	Server: DC-SIP/2.0
	Organization:

Figure 57: View audit log



Current Audit Log

```
### Reset at Thu Jan 1 00:00:00 1970 ###
### Starting Audit Thu Jan 1 00:01:13 1970 ###
### Reset at Wed Nov 9 18:14:22 2011 ###
### Starting Audit Wed Nov 9 18:14:25 2011 ###
### Reset at Wed Nov 9 18:22:41 2011 ###
### Starting Audit Wed Nov 9 18:22:43 2011 ###
### Reset at Wed Nov 9 18:24:00 2011 ###
### Starting Audit Wed Nov 9 18:24:02 2011 ###
Line 2 - Wed Nov 9 18:24:42 2011 Answer 2012029926,"9926" Duration 0 minutes 6 seconds
Line 1 - Wed Nov 9 18:24:42 2011 Call 2029927# Duration 0 minutes 6 seconds
Line 1 - Wed Nov 9 18:28:18 2011 Call *742029927 Duration 0 minutes 2 seconds
Line 1 - Wed Nov 9 18:28:43 2011 Call *742#2 Duration 0 minutes 2 seconds
Line 1 - Wed Nov 9 18:29:47 2011 Call *7422029927 Duration 0 minutes 1 seconds
Line 1 Duration 0 minutes 0 seconds
Line 2 Duration 0 minutes 0 seconds
Line 1 Duration 0 minutes 0 seconds
Line 2 Duration 0 minutes 0 seconds
```

3 CONFIGURATION

The following sections describe fundamental information about the zNID 24xx:

- Interfaces, page 86
- Factory default VLAN definition, page 87

The Configuration pages section describes the interfaces and all UI elements:

- Configuration pages, page 89

The Deployment scenarios section is a task based section which describes how to create data, video and voice connections, as well as set data services such as rate limiting, and other Network Address Translation (NAT) and DHCP services.

- Deployment scenarios, page 156
  - Creating data connections, page 162
  - Creating bridge connections, page 163
  - Creating routed connections, page 166
  - Creating brouted connections, page 172
  - Creating PPPoE tunnels, page 179
  - Creating wireless connections, page 188
  - Creating voice connections, page 191

Advanced features on page 197 describes VLANs, TLS, NAT, DHCP, rate limiting and priority setting:

- VLANS, page 197
- S-Tagged, page 200
- TLS mode, page 202
- NAT and DHCP, page 205
- DHCP server, page 209
- Data services, page 210
  - Rate limiting, page 210
  - CoS, page 211
  - Precedence, page 212

Interfaces

Interface naming conventions

zNID 24xx ONUs will support the following default interface names for the physical interfaces:

- **eth0** — Fiber WAN interface (either GPON or GigE)
- **eth1** — GigE port 1
- **eth2** — GigE port 2
- **eth3** — GigE port 3
- **eth4** — GigE port 4
- **wl0** — Wireless LAN SSID 0
- **wl0_1** — Wireless LAN SSID 1
- **wl0_2** — Wireless LAN SSID 2
- **wl0_3** — Wireless LAN SSID 3

✓ **Note:** The type and number of interfaces depends on the model of the zNID. See *zNID 24xx models and interfaces* on page 17 for more information.

Ethernet port

The ONU has a default IP address of 192.168.1.1 on the LAN Ethernet ports. The user can connect a standard PC to the LAN ports (eth1-eth4) and configure the ONU using a standard web browser. The PC will need to have an IP address on the same subnet. Typically, 192.168.1.100 is used. Of course, if you change the IP address of the ONU, you will lose connectivity. You would then need to reconfigure your PC to be on the same subnet.

See *Logging in on the Ethernet ports* on page 29.

Factory default VLAN definition

Table 31 shows the VLANs set as the factory defaults

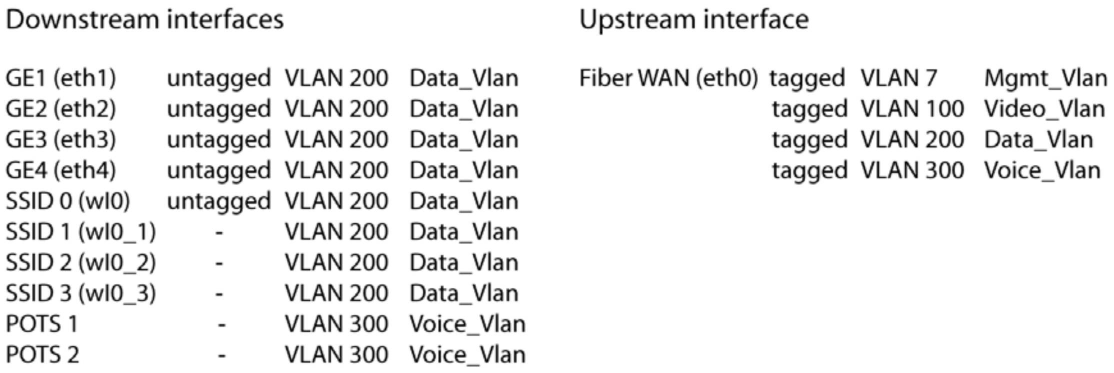
Table 31: Factory default VLANs

VLAN	Type	Tagged/Untagged	Port	IP address
7	Bridged	Tagged	eth0 (Fiber WAN – GPON or GigE)	DHCP enabled
100	Bridged	Tagged	eth0 (Fiber WAN – GPON or GigE)	n/a
200	Bridged	Tagged	eth0 (Fiber WAN – GPON or GigE)	n/a
200	Bridged	Untagged	GE1 to GE4 (GigE)	Static, 192.168.1.1
300	Bridged	Tagged	eth0 (Fiber WAN – GPON or GigE)	n/a

VLAN 7 is the default management VLAN. The fiber uplink ports are tagged members of this VLAN. The ONU is also configured to have DHCP enabled on VLAN 7. With this arrangement, the 24xx can be connected to the MXK and is ready to be remotely managed on VLAN 7 and pass data on VLAN 200 without any further configuration needed on the 24xx.

All downstream gigabit Ethernet interfaces have the Port VLAN ID (PVID) set to 200 by default. VLAN 200, the default data VLAN is also set as the PVID for the wireless SSID 0 (wl0).

Figure 58: Default VLAN and port interface settings



Downstream interfaces

GE1 (eth1)	untagged	VLAN 200	Data_Vlan
GE2 (eth2)	untagged	VLAN 200	Data_Vlan
GE3 (eth3)	untagged	VLAN 200	Data_Vlan
GE4 (eth4)	untagged	VLAN 200	Data_Vlan
SSID 0 (wl0)	untagged	VLAN 200	Data_Vlan
SSID 1 (wl0_1)	-	VLAN 200	Data_Vlan
SSID 2 (wl0_2)	-	VLAN 200	Data_Vlan
SSID 3 (wl0_3)	-	VLAN 200	Data_Vlan
POTS 1	-	VLAN 300	Voice_Vlan
POTS 2	-	VLAN 300	Voice_Vlan

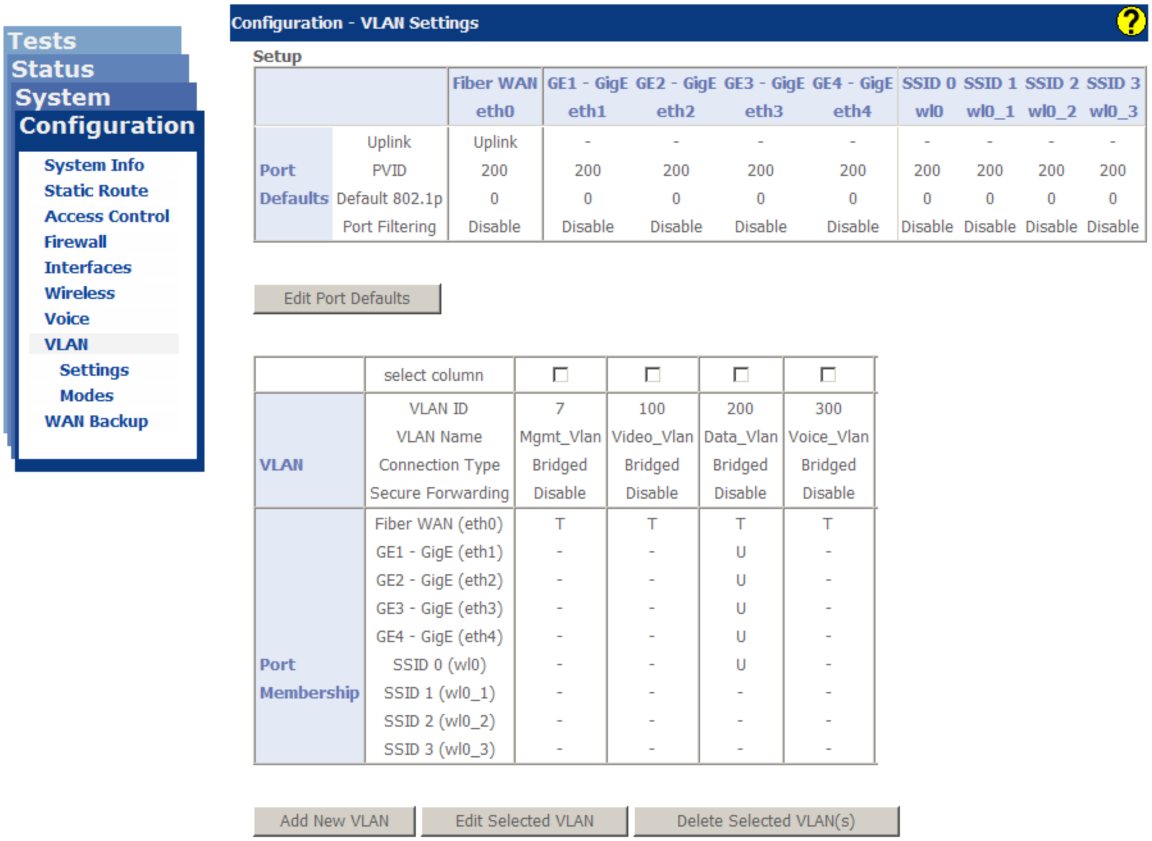
Upstream interface

Fiber WAN (eth0)	tagged	VLAN 7	Mgmt_Vlan
	tagged	VLAN 100	Video_Vlan
	tagged	VLAN 200	Data_Vlan
	tagged	VLAN 300	Voice_Vlan

For more information about PVID see *Edit Port Defaults* on page 145.

Figure 59 shows how the default interfaces from Figure 58 and Figure 31 are displayed in the Web UI.

Figure 59: Default VLANs and interfaces as displayed in the Configuration | VLAN | Settings page



Configuration - VLAN Settings

Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSID 2 wl0_2	SSID 3 wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	PVID	200	200	200	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0	0
	Port Filtering	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable

	select column	□	□	□	□
VLAN	VLAN ID	7	100	200	300
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	Connection Type	Bridged	Bridged	Bridged	Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-
	GE2 - GigE (eth2)	-	-	U	-
	GE3 - GigE (eth3)	-	-	U	-
	GE4 - GigE (eth4)	-	-	U	-
	SSID 0 (wl0)	-	-	U	-
	SSID 1 (wl0_1)	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-
	SSID 3 (wl0_3)	-	-	-	-

The VLAN to associate with the POTS interfaces is the **Bound Interface Name** parameter in the **Configuration | Voice | SIP** page or the **Configuration | Voice | MGCP** pages. The POTS interfaces are not show on the **Configuration | VLAN | Settings** page.

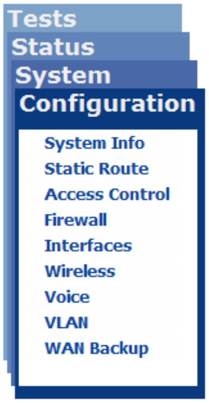
Configuration pages

The Configuration Menu has the screens for configuring interfaces. This section describes the following pages of the Web user interface:

- System info, page 90
- Static route, page 91
- Access control, page 92
- Firewall, page 94
- Interfaces, page 100
- Wireless, page 108
- Voice, page 134
- VLAN, page 143
- WAN backup, page 153

See Deployment scenarios, page 156 for procedures for the different scenarios which can be configured using these configuration pages.

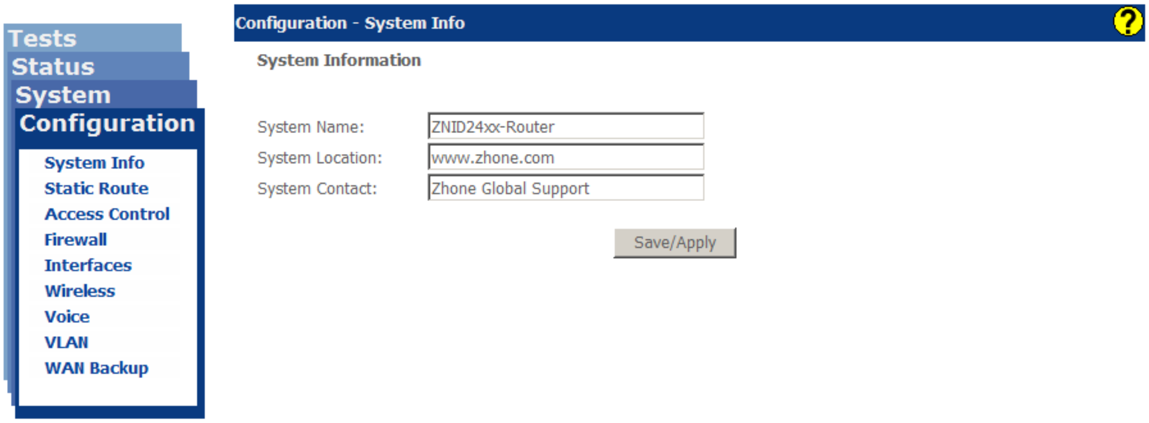
Figure 60: The configuration menu



System info

The **Configuration | System Info** page provides the mechanism for setting the MIB-2 SNMP objects for **System Name**, **System Location** and **System Contact**. The **System Name** is also in the screen banner. If you change the System name, to get the **System Name** to update in the banner click refresh on the browser.

Figure 61: Setting system information.



Configuration - System Info

System Information

System Name: ZNID24xx-Router

System Location: www.zhone.com

System Contact: Zhone Global Support

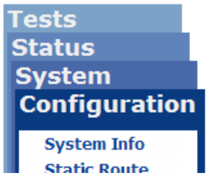
Table 32: Device Info page display

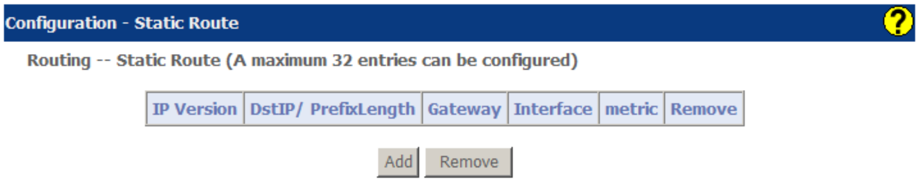
UI Label	Description
System Name	**System Name** is a user definable name which can be used to identify the ONU. The **System Name** is used in the banner for the Web User Interface for the ONU. **System Name** is the MIB-2 object, SysName.
System Location	**System Location** is user definable information to help identify the ONU and the location of the ONU. System Location is the MIB-2 object, sysLocation.
System Contact	**System Contact** is user definable information to help identify the ONU and who to contact about the system. **System Contact** is the MIB-2 object, SysContact

Static route

The **Configuration | Static Route** page provides the mechanism for adding static routes to the zNID.

Figure 62: The Static Route page has a table of static routes



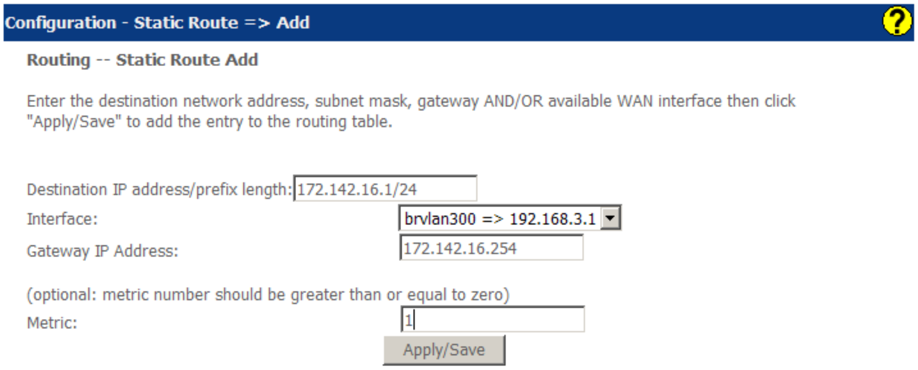

Configuration - Static Route

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

To add a route, click **Add**.

Figure 63: Adding a static route


Configuration - Static Route => Add

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

Destination IP address/prefix length: 172.142.16.1/24

Interface: brvlan300 => 192.168.3.1

Gateway IP Address: 172.142.16.254

(optional: metric number should be greater than or equal to zero)

Metric: 1

Table 33: Adding a static route

UI Label	Description
Destination IP address	The IP address of the destination device. This field will accept an IP address/n notation where the “/n” represents the number of bits for creating a network mask. For example a net mask of 255.255.255.0 is 24 bits and would be designated by a “/24”
Interface	The LAN interface for the static route
Gateway IP Address	The IP address of the default gateway for the subnet in which the zNID resides.
Metric	Defines the number of hops to the destination. The metric must be 0 or greater.

Access control

Access control lists define whether packets/frames from source IP addresses or source MAC addresses are allowed in on an interface.

Note that firewall rules, access control and port forwarding, require the firewall feature to be enabled.

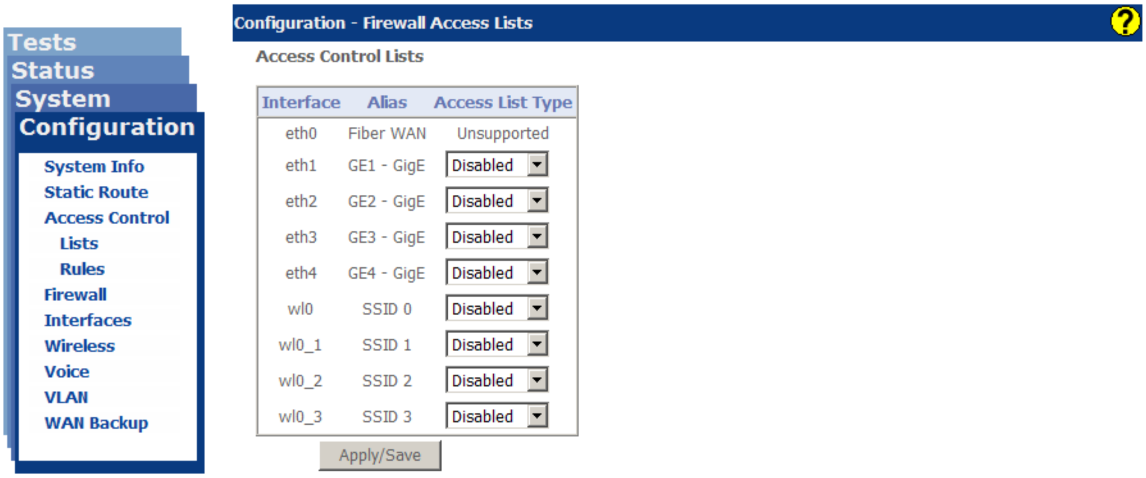
Lists

There are three options for defining whether packets/frames will be allowed in on an interface — disabled, black list and white list. An interface may only have one of the three listing options:

- Black list defines a set of source IP addresses/MAC addresses which will not be allowed. All other packets will be allowed.
- White list defines a set of source IP addresses/MAC addresses which will be allowed. All other packets will be blocked.
- Disabled allows all packets/frames.

The Fiber WAN uplink is unsupported because filtering is not allowed on this interface.

Figure 64: Defining whether the interface will be disabled, have a black list or a white list



Configuration - Firewall Access Lists

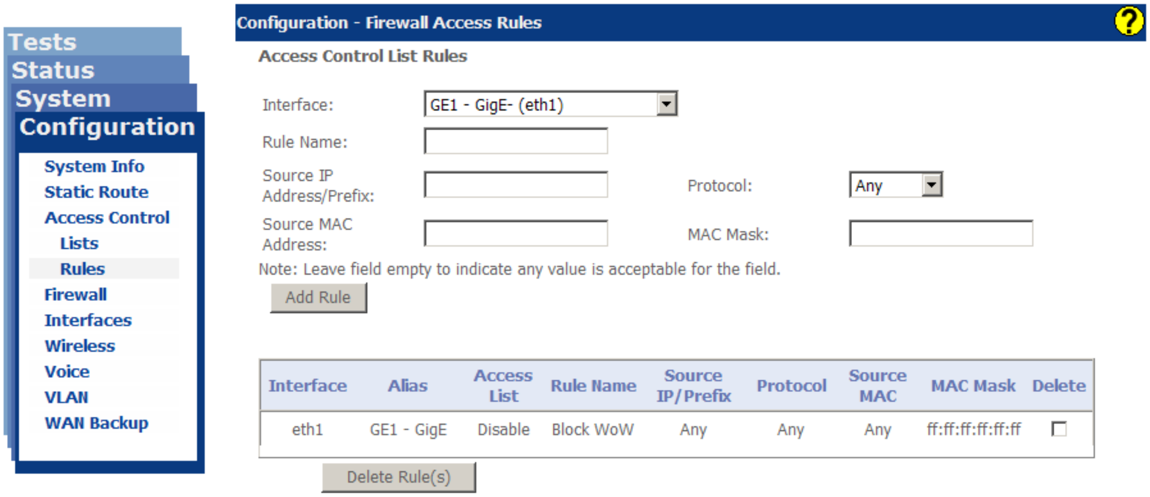
Access Control Lists

Interface	Alias	Access List Type
eth0	Fiber WAN	Unsupported
eth1	GE1 - GigE	Disabled
eth2	GE2 - GigE	Disabled
eth3	GE3 - GigE	Disabled
eth4	GE4 - GigE	Disabled
wl0	SSID 0	Disabled
wl0_1	SSID 1	Disabled
wl0_2	SSID 2	Disabled
wl0_3	SSID 3	Disabled

Rules

The **Configuration|Access Control|Rules** page defines the access control list rules.

Figure 65: Defining the rules for access list



Configuration - Firewall Access Rules

Access Control List Rules

Interface: GE1 - GigE- (eth1)

Rule Name:

Source IP Address/Prefix:

Protocol: Any

Source MAC Address:

MAC Mask:

Note: Leave field empty to indicate any value is acceptable for the field.

Interface	Alias	Access List	Rule Name	Source IP/Prefix	Protocol	Source MAC	MAC Mask	Delete
eth1	GE1 - GigE	Disable	Block WoW	Any	Any	Any	ff:ff:ff:ff:ff:ff	□

Table 34: Adding an access control rule

UI Label	Description
Interface	Selects the physical interface to which the configured rule will apply. Changes made to the selection will cause the access control filtering table for the selected (and deselected) interface to change.
Rule Name	A required user defined identifier for the rule. This identifier must be unique per interface rule.
Source IP Address/ Prefix	The IP address or subnet to filter. If the Prefix is 32 then the whole address is used. Otherwise the prefix indicates the subnet to filter against. Example: 192.168.1.0/24 would filter against the 192.168.1 subnet.
Protocol	Select either ICMP, IGMP, TCP or UDP.
Source MAC Address	The MAC address to filter. MAC addresses have the format AA:BB:CC:DD:EE:FF.
MAC Mask	Mask by which to filter MAC address. For example a MAC Mask of ff:ff:ff:00:00:00 would filter against the first six digits of the MAC address.

To define an access control rule

1. Select the interface to which to apply the rule
2. Enter a unique rule name in the **Rule Name** text box
3. Define the Source IP address, subnet, MAC address or MAC mask for the rule
4. Click **Add Rule**

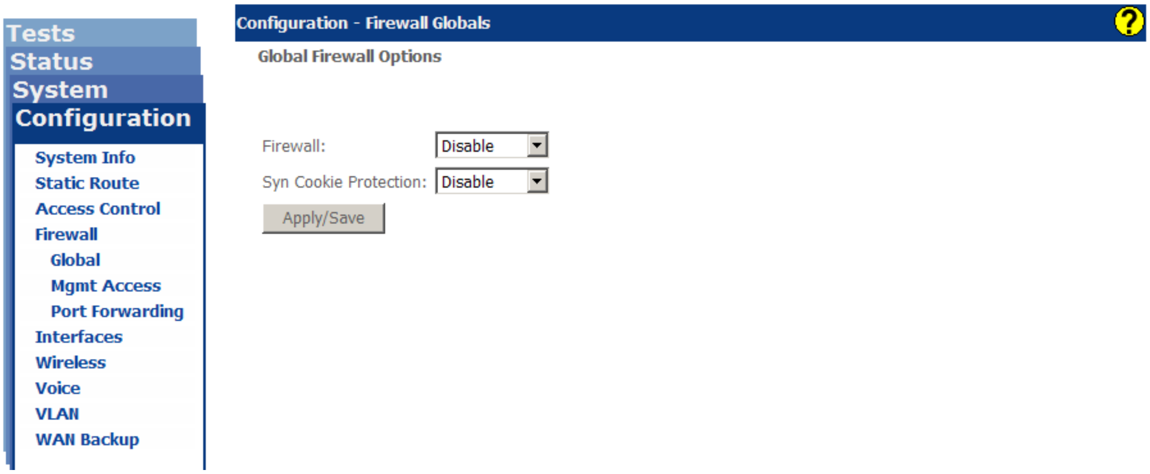
Firewall

The firewall in the zNID 24xx provides protection against unwanted intrusion.

Global

The **Firewall | Global** page mainly enables the firewall options — management access and port forwarding. The Firewall dropdown must have **Enable** selected for management access and port forwarding to be active.

Figure 66: Top level firewall options



Configuration - Firewall Globals

Global Firewall Options

Firewall: Disable

Syn Cookie Protection: Disable

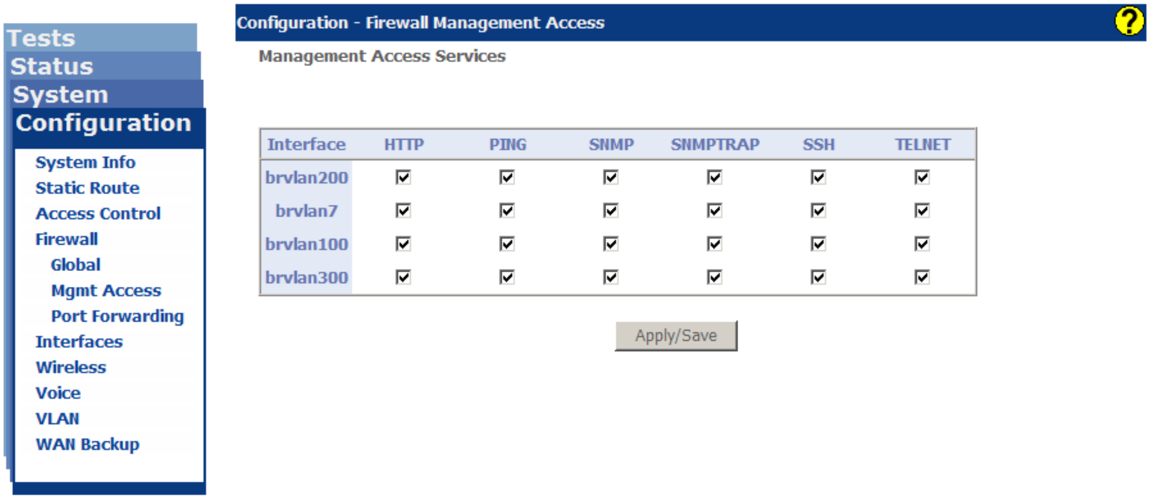
Syn Cookie Protection protects against malicious attackers attempting to exploit TCP handshaking.

Management access

The Firewall Management Access table lists all the interfaces for which management traffic can be received. A check under the protocol indicates that this protocol is Allowed on the interface.

The firewall global option must be enabled before this screen will take effect.

Figure 67: Firewall management port access table



Interface	HTTP	PING	SNMP	SNMPTRAP	SSH	TELNET
brvlan200	☑	☑	☑	☑	☑	☑
brvlan7	☑	☑	☑	☑	☑	☑
brvlan100	☑	☑	☑	☑	☑	☑
brvlan300	☑	☑	☑	☑	☑	☑

Table 35: Management services

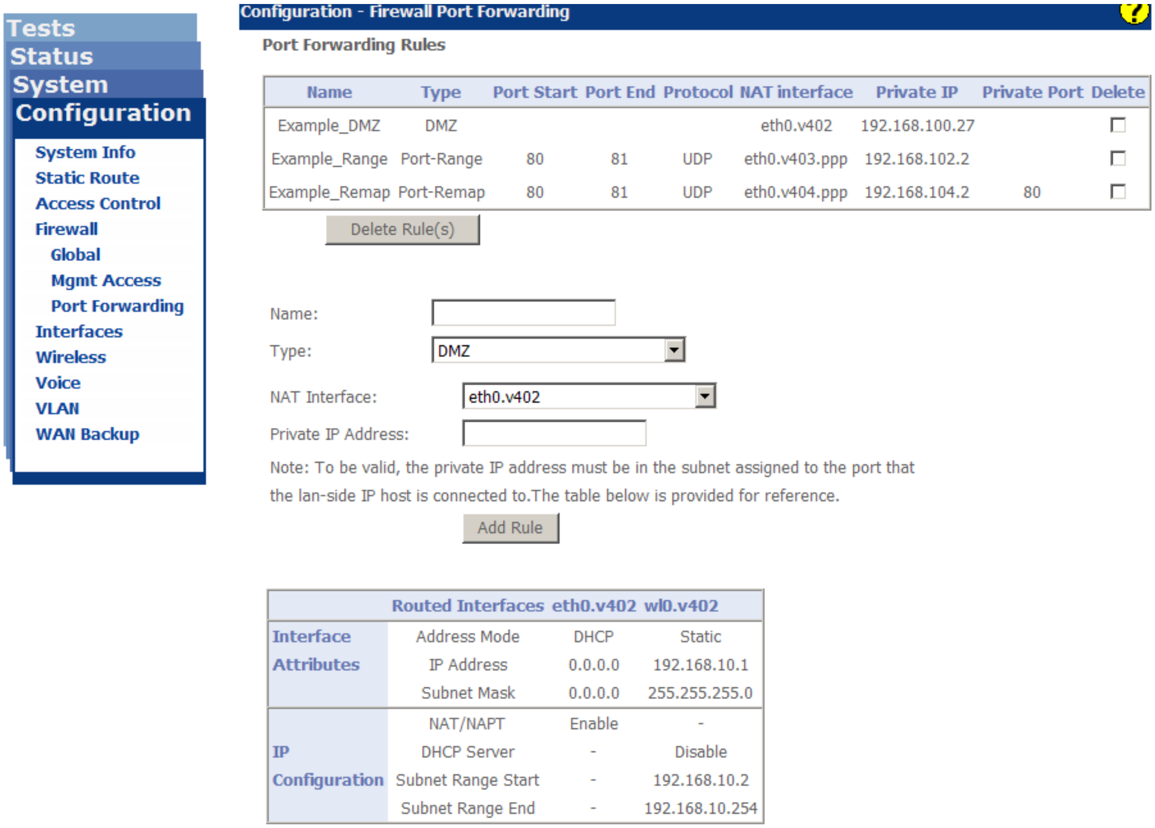
UI Label	Description
Interface	The VLAN interface.
HTTP	Web Browser Traffic.
PING	ICMP Echoes used to test for connectivity.
SNMP	Simple Network Management Protocol.
SNMPTRAP	Alarms for Simple Network Management Protocol.
SSH	Secure Shell.
TELNET	Remote Terminal support.

Port forwarding

The top table of the **Port Forwarding** screen reflects the existing port forwarding rules. As Rules are added, the top table displays those changes. The Delete Rule(s) button allows one or more rules to be removed from the ONU.

The bottom table reflects the values that have been configured (Configuration/Interfaces/Routed or Configuration/Interfaces/PPPoE) for the selected interface. The table is refreshed when a new interface is selected.

Figure 68: The table at the top shows the current port forwarding rules. Define the port forwarding rules at the bottom of the page



Port Forwarding Rules

Name	Type	Port Start	Port End	Protocol	NAT interface	Private IP	Private Port	Delete
Example_DMZ	DMZ				eth0.v402	192.168.100.27		□
Example_Range	Port-Range	80	81	UDP	eth0.v403.ppp	192.168.102.2		□
Example_Remap	Port-Remap	80	81	UDP	eth0.v404.ppp	192.168.104.2	80	□

Name:	
Type:	DMZ
NAT Interface:	eth0.v402
Private IP Address:	

Note: To be valid, the private IP address must be in the subnet assigned to the port that the lan-side IP host is connected to.The table below is provided for reference.

	Routed Interfaces	eth0.v402	wl0.v402
Interface Attributes	Address Mode	DHCP	Static
	IP Address	0.0.0.0	192.168.10.1
	Subnet Mask	0.0.0.0	255.255.255.0
IP Configuration	NAT/NAPT	Enable	-
	DHCP Server	-	Disable
	Subnet Range Start	-	192.168.10.2
	Subnet Range End	-	192.168.10.254

Table 36: Defining port forwarding rules

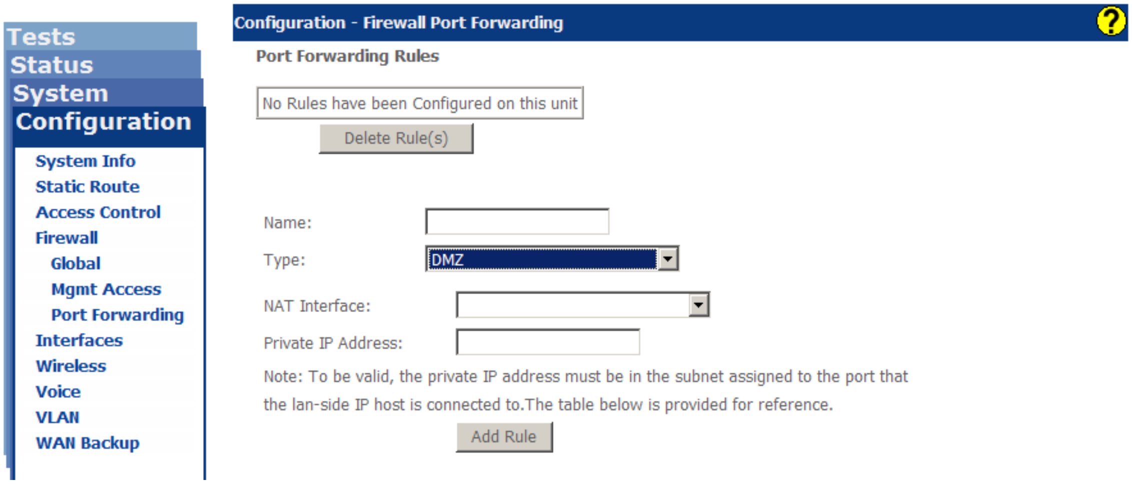
UI Label	Description
Name	User defined name to identify rule.
Type	• **DMZ** When DMZ is chosen it is the only rule allowed on that interface. A DMZ rule is effectively the same as a Range rule with all ports included. • **Range** Range rules are more secure than setting a DMZ rule, because Range rules allow specific ports or groups of ports to be opened up. Range indicates that any traffic on those ports will be sent to the private IP address. • **Remap** Remap indicates that any traffic on those ports will be sent to the private IP address at the private port.
Port Start	Lowest value port number for the range.
Port End	Highest value port number for the range. This can be equal to Port Start if there is only one port.
Protocol	TCP, UDP or Both indicate which protocols to monitor for the port numbers.
NAT Interface	The Interface to monitor for this rule.
Private IP Address	The IP address to which to send the traffic.
Port	The Port address to which to send the traffic.

The **Add Rule** button will save the configured rule if valid. NOTE: these rules have no effect until the global firewall option is enabled.

Defining port forwarding rules

1. Be sure that **Firewall** is set to **Enabled** on the **Firewall | Global** page
2. In the **Name** text box enter a name for the rule
3. From the **Type** dropdown select the type of port forwarding rule
4. Enter the appropriate information for the rule (depends on rule type)
5. Click **Add Rule**

Figure 69: DMZ rule



Configuration - Firewall Port Forwarding

Port Forwarding Rules

No Rules have been Configured on this unit

Name:

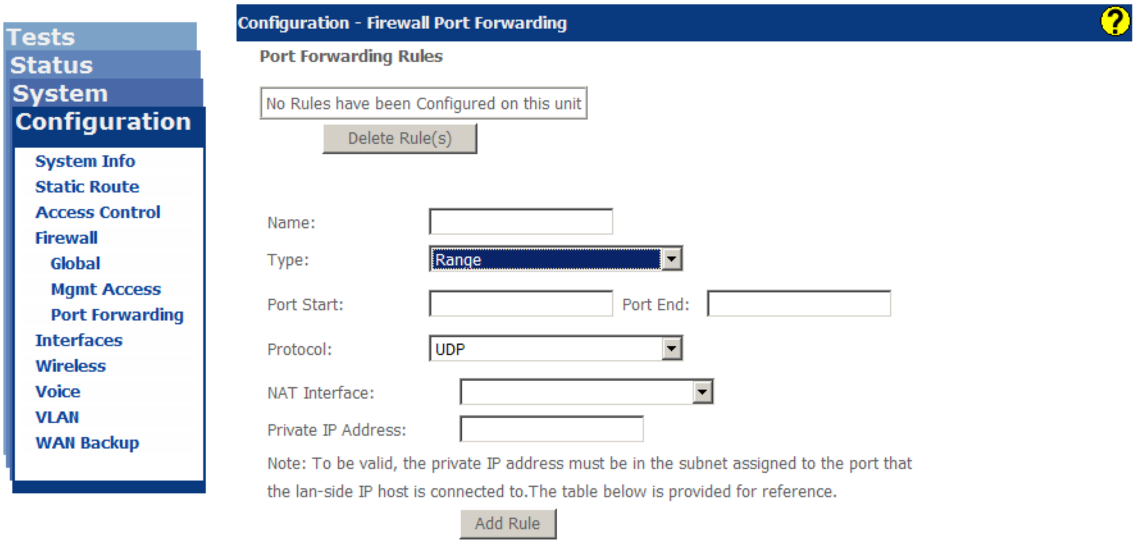
Type: DMZ

NAT Interface:

Private IP Address:

Note: To be valid, the private IP address must be in the subnet assigned to the port that the lan-side IP host is connected to.The table below is provided for reference.

Figure 70: Port forwarding range rule



Configuration - Firewall Port Forwarding

Port Forwarding Rules

No Rules have been Configured on this unit

Name:

Type: Range

Port Start: Port End:

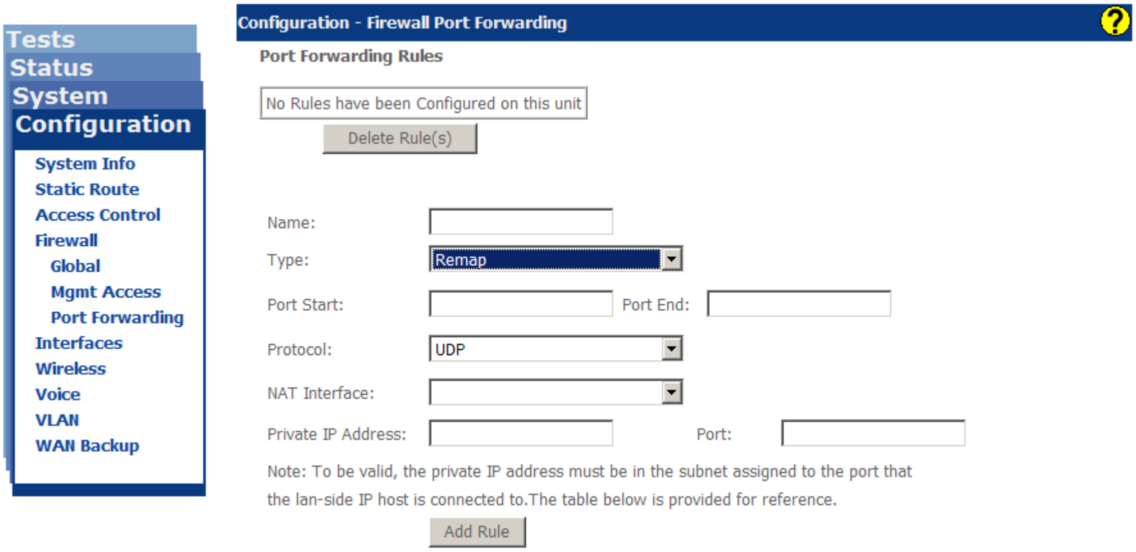
Protocol: UDP

NAT Interface:

Private IP Address:

Note: To be valid, the private IP address must be in the subnet assigned to the port that the lan-side IP host is connected to.The table below is provided for reference.

Figure 71: Port forwarding remap rule



Configuration - Firewall Port Forwarding

Port Forwarding Rules

No Rules have been Configured on this unit

Name:

Type: Remap

Port Start: Port End:

Protocol: UDP

NAT Interface:

Private IP Address: Port:

Note: To be valid, the private IP address must be in the subnet assigned to the port that the lan-side IP host is connected to.The table below is provided for reference.

Interfaces

The Zhone zNIDs support a variety of interface types:

- *Bridged* on page 100
- *Routed* on page 101
- *Brouted* on page 102
- *PPPoE* on page 103
- *Ethernet* on page 104
- *GPON* on page 106

Rate limiting is also available for the WAN and LAN Ethernet interfaces. See *Rate Limits* on page 107

Bridged

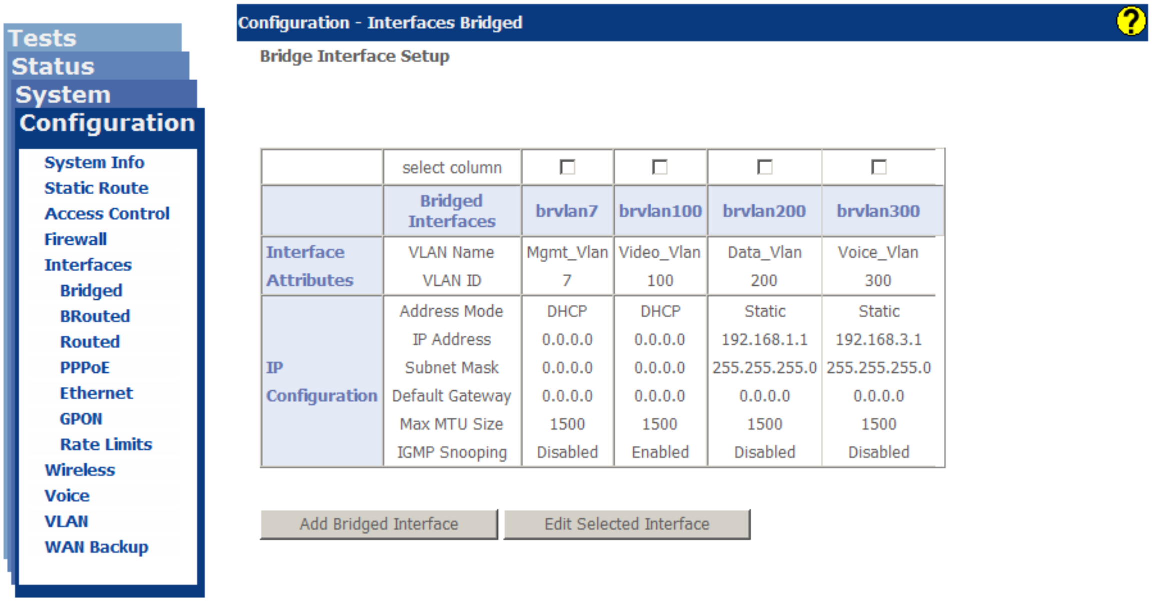
Bridges are ISO layer two functions which connect network segments and direct traffic based on Ethernet Media Access Control (MAC) addresses. MAC addresses are a unique address per physical device. Routers are layer three devices which use IP Addresses to direct packets.

Bridges direct packets based on address information in the packets as well as information learned from the processing and directing of other packets.

The **Interfaces | Bridged** page displays the bridged interfaces which have been defined and the IP address assigned to that interface.

To create bridge interfaces see Creating bridge connections, page 163.

Figure 72: The Configuration | Bridges page, shows existing bridges by VLAN.



Configuration - Interfaces Bridged

Bridge Interface Setup

	select column	□	□	□	□
	Bridged Interfaces	brvlan7	brvlan100	brvlan200	brvlan300
Interface Attributes	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	VLAN ID	7	100	200	300
IP Configuration	Address Mode	DHCP	DHCP	Static	Static
	IP Address	0.0.0.0	0.0.0.0	192.168.1.1	192.168.3.1
	Subnet Mask	0.0.0.0	0.0.0.0	255.255.255.0	255.255.255.0
	Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
	Max MTU Size	1500	1500	1500	1500
	IGMP Snooping	Disabled	Enabled	Disabled	Disabled

To edit a bridge, enter a check in the bridged interface in the select row at the top of the table, then click **Edit Selected Interface**.

The table displays Bridged Interfaces along with any IP Addresses that have been assigned to them for the purposes of enabling management access or supporting SIP, SIP-PLAR or MGCP clients. The naming convention for Bridged Interfaces is “brvlan” followed by the VLAN ID. Bridged Interfaces are automatically sorted and displayed in ascending VLAN ID order.

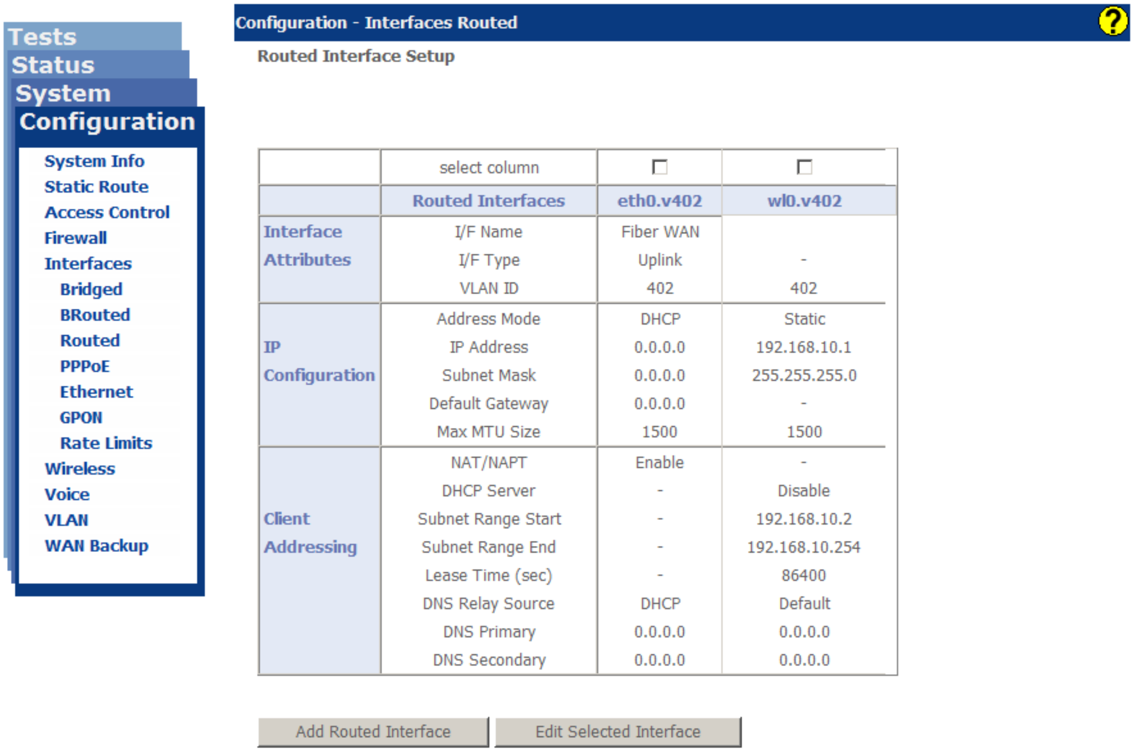
Routed

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite.

The **Interfaces | Routed** page displays the routed interfaces which have been defined and the IP address assigned to that interface.

To create routed interfaces see Creating routed connections, page 166

Figure 73: Routed interfaces



Configuration - Interfaces Routed

Routed Interface Setup

	select column	□	□
	Routed Interfaces	eth0.v402	wl0.v402
Interface Attributes	I/F Name	Fiber WAN	
	I/F Type	Uplink	-
	VLAN ID	402	402
IP Configuration	Address Mode	DHCP	Static
	IP Address	0.0.0.0	192.168.10.1
	Subnet Mask	0.0.0.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	Enable	-
	DHCP Server	-	Disable
	Subnet Range Start	-	192.168.10.2
	Subnet Range End	-	192.168.10.254
	Lease Time (sec)	-	86400
	DNS Relay Source	DHCP	Default
	DNS Primary	0.0.0.0	0.0.0.0
	DNS Secondary	0.0.0.0	0.0.0.0

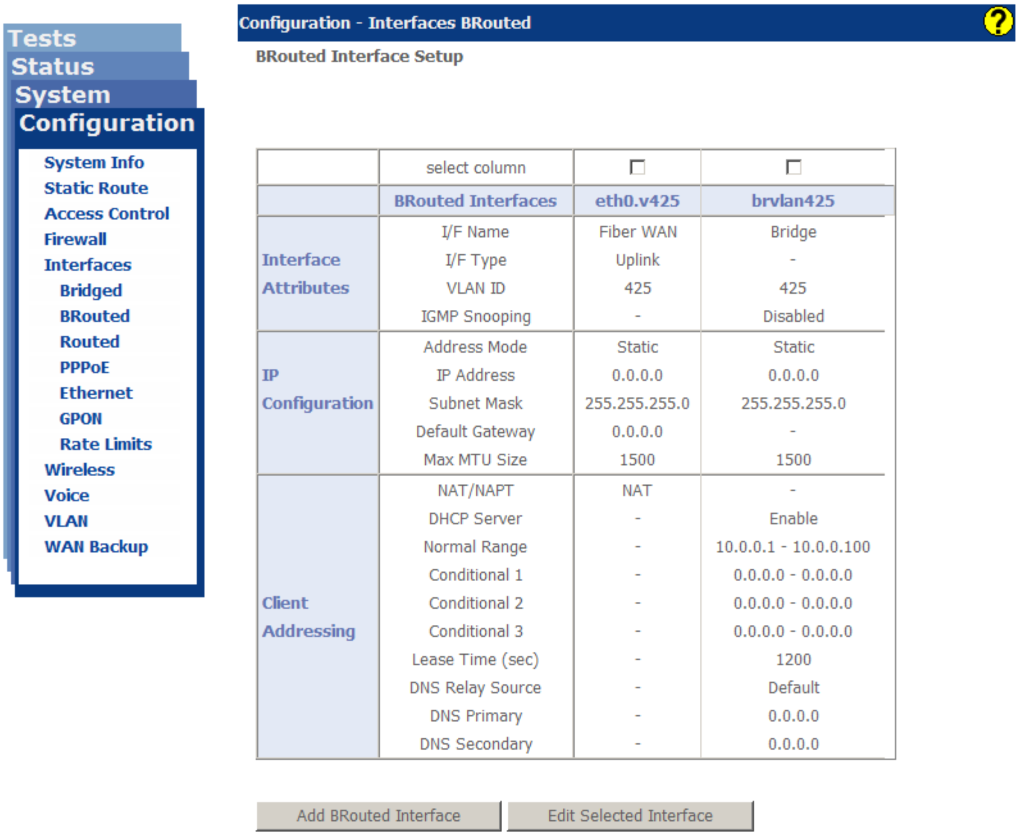
To edit a routed interface, enter a check in the routed interface in the select row at the top of the table, then click **Edit Selected Interface**.

Brouted

Brouted VLANs have two IP interfaces — one for the Routed uplink interface and a second for the Bridged LAN-side interface. A Brouted VLAN may have multiple LAN ports as members, and all ports will use the same IP subnet. So Brouted means that the LAN side is like a bridge, but has a routed interface for the WAN side.

To create brouted interfaces see Creating brouted connections, page 172.

Figure 74:



Configuration - Interfaces BRouted

BRouted Interface Setup

	select column	☐	☐
	BRouted Interfaces	eth0.v425	brvlan425
Interface Attributes	I/F Name	Fiber WAN	Bridge
	I/F Type	Uplink	-
	VLAN ID	425	425
	IGMP Snooping	-	Disabled
IP Configuration	Address Mode	Static	Static
	IP Address	0.0.0.0	0.0.0.0
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	NAT	-
	DHCP Server	-	Enable
	Normal Range	-	10.0.0.1 - 10.0.0.100
	Conditional 1	-	0.0.0.0 - 0.0.0.0
	Conditional 2	-	0.0.0.0 - 0.0.0.0
	Conditional 3	-	0.0.0.0 - 0.0.0.0
	Lease Time (sec)	-	1200
	DNS Relay Source	-	Default
	DNS Primary	-	0.0.0.0
	DNS Secondary	-	0.0.0.0

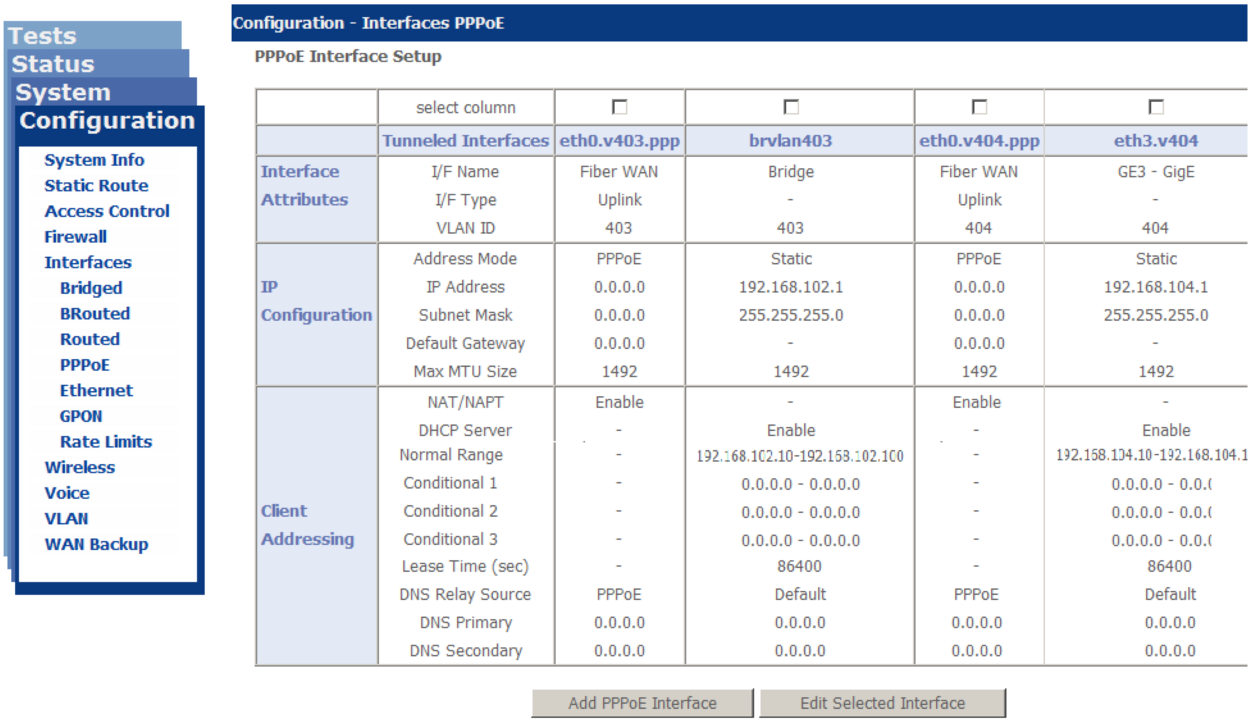
PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) encapsulates PPP frames inside Ethernet frames to create a PPPoE tunnel between hosts connected to the ZNID and other devices out in the cloud. While Ethernet is packet-based (so no direct connection is opened), PPP is a direct connection where one device directly connects to another using the protocol. PPPoE is a virtual connection (usually called tunnel) between two devices.

On the **Configuration | Interfaces | PPPoE** page you can add a PPPoE on a port by VLAN, either as **PPPoE Routed** or **PPPoE Bridged**.

To create PPPoE tunnels see Creating PPPoE tunnels, page 179

Figure 75: The PPPoE Interface Setup page



Configuration - Interfaces PPPoE

PPPoE Interface Setup

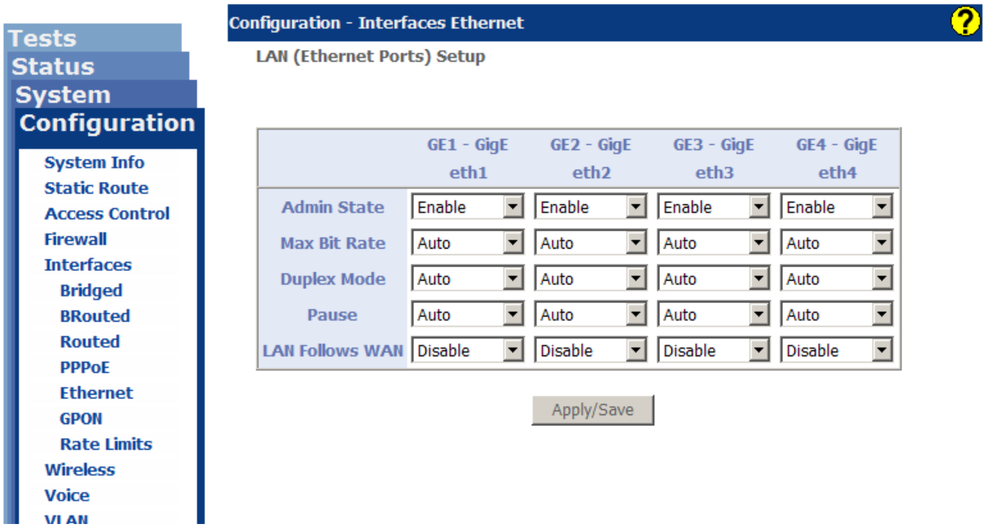
	select column	□	□	□	□
	Tunneled Interfaces	eth0.v403.ppp	brvlan403	eth0.v404.ppp	eth3.v404
Interface Attributes	I/F Name	Fiber WAN	Bridge	Fiber WAN	GE3 - GigE
	I/F Type	Uplink	-	Uplink	-
	VLAN ID	403	403	404	404
IP Configuration	Address Mode	PPPoE	Static	PPPoE	Static
	IP Address	0.0.0.0	192.168.102.1	0.0.0.0	192.168.104.1
	Subnet Mask	0.0.0.0	255.255.255.0	0.0.0.0	255.255.255.0
	Default Gateway	0.0.0.0	-	0.0.0.0	-
	Max MTU Size	1492	1492	1492	1492
Client Addressing	NAT/NAPT	Enable	-	Enable	-
	DHCP Server	-	Enable	-	Enable
	Normal Range	-	192.168.102.10-192.168.102.100	-	192.168.104.10-192.168.104.1
	Conditional 1	-	0.0.0.0 - 0.0.0.0	-	0.0.0.0 - 0.0.(
	Conditional 2	-	0.0.0.0 - 0.0.0.0	-	0.0.0.0 - 0.0.(
	Conditional 3	-	0.0.0.0 - 0.0.0.0	-	0.0.0.0 - 0.0.(
	Lease Time (sec)	-	86400	-	86400
	DNS Relay Source	PPPoE	Default	PPPoE	Default
	DNS Primary	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
	DNS Secondary	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

To edit a routed interface, enter a check in the routed interface in the select row at the top of the table, then click **Edit Selected Interface**.

Ethernet

The **Interfaces | Ethernet** page provides the mechanism to modify Ethernet parameters for Ethernet interfaces.

Figure 76: Ethernet parameters



Configuration - Interfaces Ethernet

LAN (Ethernet Ports) Setup

	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4
Admin State	Enable	Enable	Enable	Enable
Max Bit Rate	Auto	Auto	Auto	Auto
Duplex Mode	Auto	Auto	Auto	Auto
Pause	Auto	Auto	Auto	Auto
LAN Follows WAN	Disable	Disable	Disable	Disable

Table 37: Ethernet settings

UI Label	Description
Admin State	• **Enable -** Port is enabled and a link has been established • **Disable -** Port is disabled (administratively down) • **NoLink -** Ethernet Port is enabled, but no device is connected
Max Bit Rate	The maximum possible bit rate of the physical layer • **10** - 10 Mbps • **100** - 100 Mbps • **1000** - 1000 Mbps • **Auto**
Duplex Mode	Full or Half Duplex
Pause	In Ethernet flow control, a pause frame request stopping transmission, so the receiving device can catch up. • **Enable -** • **Disable -** Pause frames are disabled • **Auto -** Pause

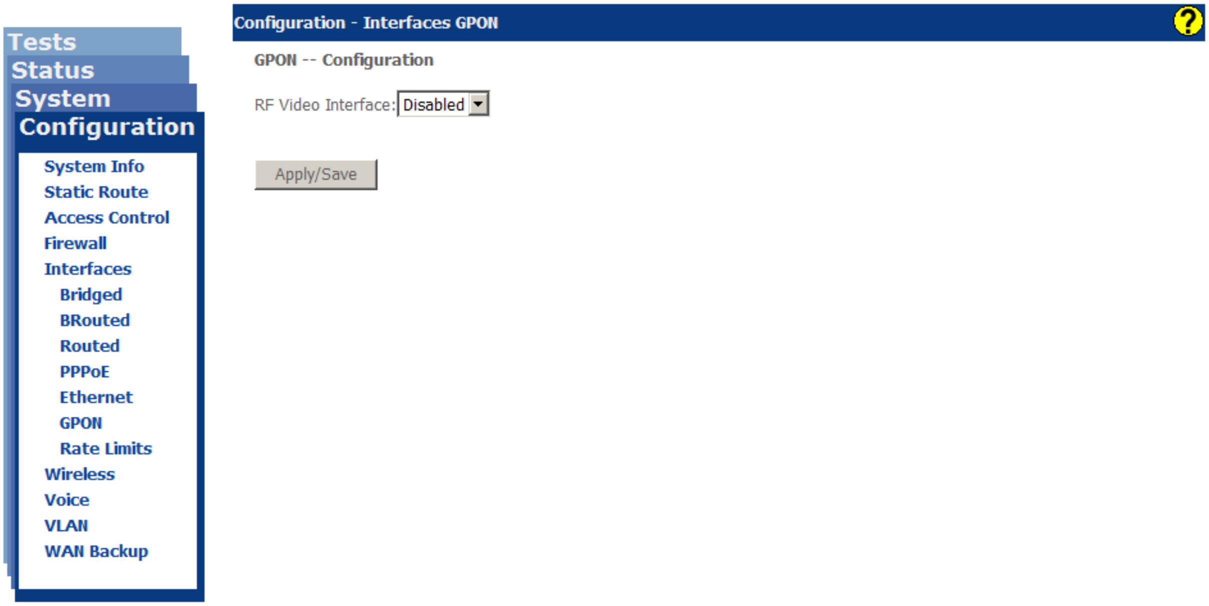
Table 37: Ethernet settings

UI Label	Description
LAN Follows WAN	When enabled, the LAN port is forced to a physical down state when the WAN uplink has been down for 15 seconds. This mechanism is used to signal to attached devices that they need to initiate a backup connection. When the WAN uplink has been back up for 30 seconds, the LAN port is re-enabled to restore service.

GPON

The **Interfaces | GPON** page allows you to enable RF video on models which support RF video.

Figure 77: RF video may be enabled or disabled



GPON -- Configuration

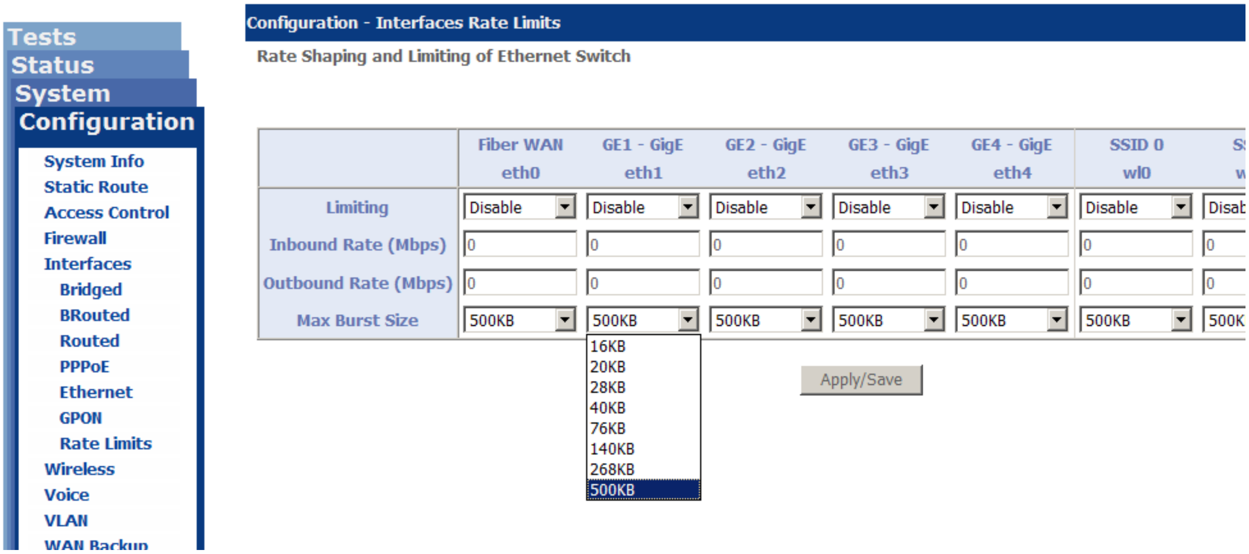
RF Video Interface: Disabled

For models which support RF video, RF video may also be disabled to conserve power when RF video is not in use.

Rate Limits

Rate limiting can be configured on the WAN uplink, LAN Ethernet interfaces, HPNA coax and HPNA phone ports.

Figure 78: Rate shaping and limiting on Ethernet ports



Configuration - Interfaces Rate Limits

Rate Shaping and Limiting of Ethernet Switch

	Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	S w
Limiting	Disable	Disable	Disable	Disable	Disable	Disable	Disab
Inbound Rate (Mbps)	0	0	0	0	0	0	0
Outbound Rate (Mbps)	0	0	0	0	0	0	0
Max Burst Size	500KB	500KB	500KB	500KB	500KB	500KB	500K

Table 38: Rate limiting

UI Label	Description
Limiting	Limit enabled or disabled on interface.
Inbound	Rate limit inbound traffic. The supported values are 0-1000Mbps (0 disables rate limit, rate above 100Mbps must be increments of 8 starting at 104Mbps). If the allowed inbound rate is exceeded, pause frames are transmitted to the attached device. It is recommended that the attached device is configured to obey pause frames to reduce overhead caused by TCP/IP packet retransmission.
Outbound	Rate limit outbound traffic. The supported values are 1-1000Mbps (0 disables rate limit, rate above 100Mbps must be increments of 8 starting at 104Mbps). If the allowed outbound rate is exceeded, pause frames are transmitted out the source interface (ingress interface that is causing the congestion).
Max Rate Mbps	The Rate Shaping Total per interval.
Max Burst Size	The Rate Shaping Burst per interval.

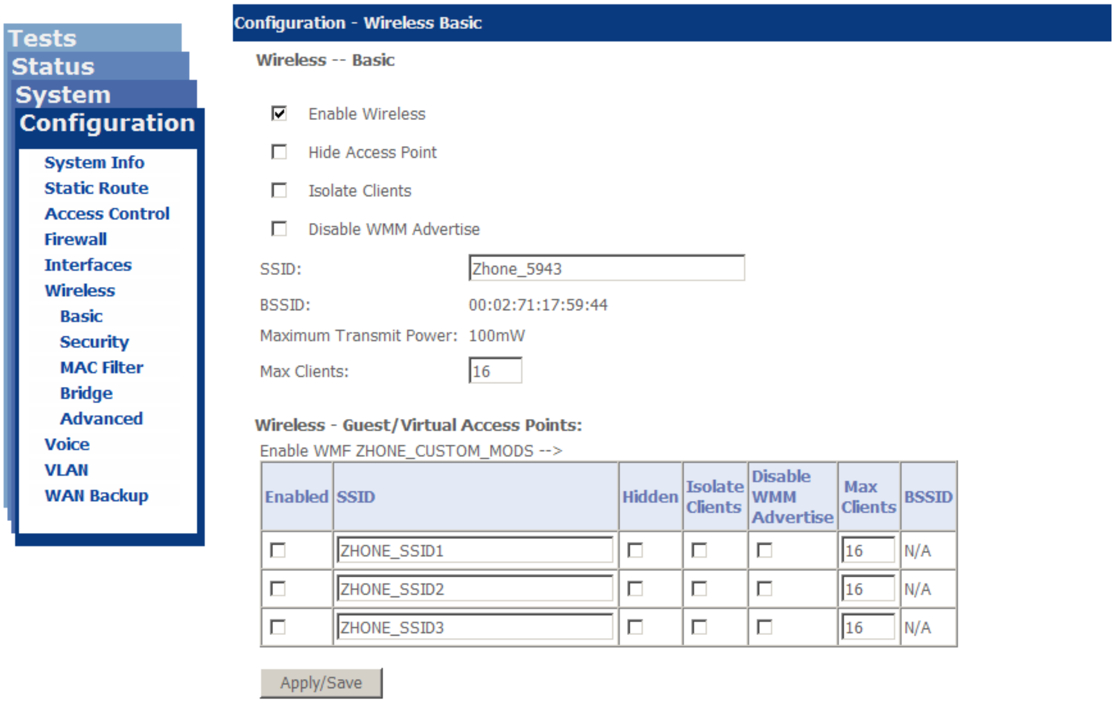
Wireless

Basic

The **Wireless | Basic** page sets the name for the network (SSID, service set identifier) which identifies the AP to clients. You also can set basic functionality such as setting the maximum number of clients which can be connected to the AP.

Other general security features such as hiding the SSID and isolating clients are also controlled from this page. More specific security measures such as defining authentication and encryption methods are described in *Security* on page 110.

Figure 79: Basic AP configuration options



Configuration - Wireless Basic

Wireless -- Basic

☑ Enable Wireless

□ Hide Access Point

□ Isolate Clients

□ Disable WMM Advertise

SSID: Zhone_5943

BSSID: 00:02:71:17:59:44

Maximum Transmit Power: 100mW

Max Clients: 16

Wireless - Guest/Virtual Access Points:

Enable WMF ZHONE_CUSTOM_MODS -->

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Max Clients	BSSID
□	ZHONE_SSID1	□	□	□	16	N/A
□	ZHONE_SSID2	□	□	□	16	N/A
□	ZHONE_SSID3	□	□	□	16	N/A

Table 39: Basic wireless settings.

UI Label	Description
Enable Wireless	Enables the wireless transceiver. To pass traffic a VLAN must be associated with the wireless interface. See *Creating wireless connections* on page 188 for creating wireless connections.
Hide Access Point	Hides the Access Point SSID from scans. To connect to the Access Point the SSID must be entered from the client.
Isolate Clients	Isolates clients within the wireless network from communicating directly with each other.

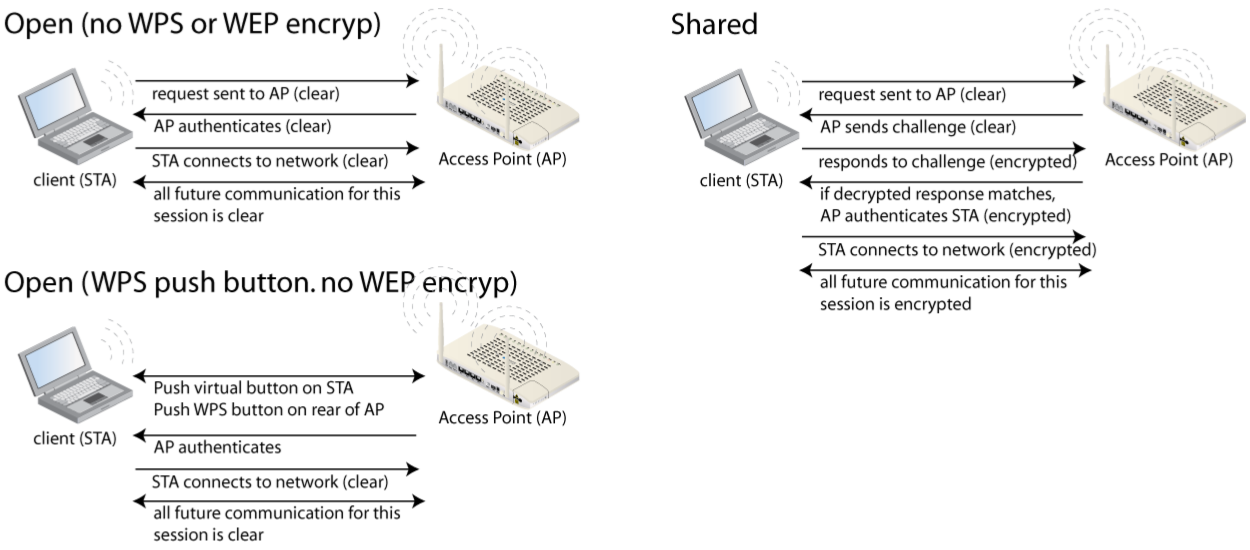
Table 39: Basic wireless settings.

UI Label	Description
Disable WMM Advertise	WMM (Wireless Multi Media) provides a subset of the IEEE 802.11e QoS standard, which adds prioritization to wireless to optimize their performance. When multiple concurrent applications are on the wireless network each application may have different latency and throughput needs. WMM provides for this optimization, however WMM may provide slower performance for some applications.
SSID	Service Set Identifier identifies the wireless LAN to clients. The SSID is a customer definable name for the AP, but must be unique.
BSSID	Basic Service Set Identifier is a unique identifier which identifies the AP. Essentially a MAC address for the AP and is not configurable.
Country	Selects the channel set based on country requirements.
Max Clients	Sets the number of clients allowed on the wireless network. The maximum number of clients is 16.

Security

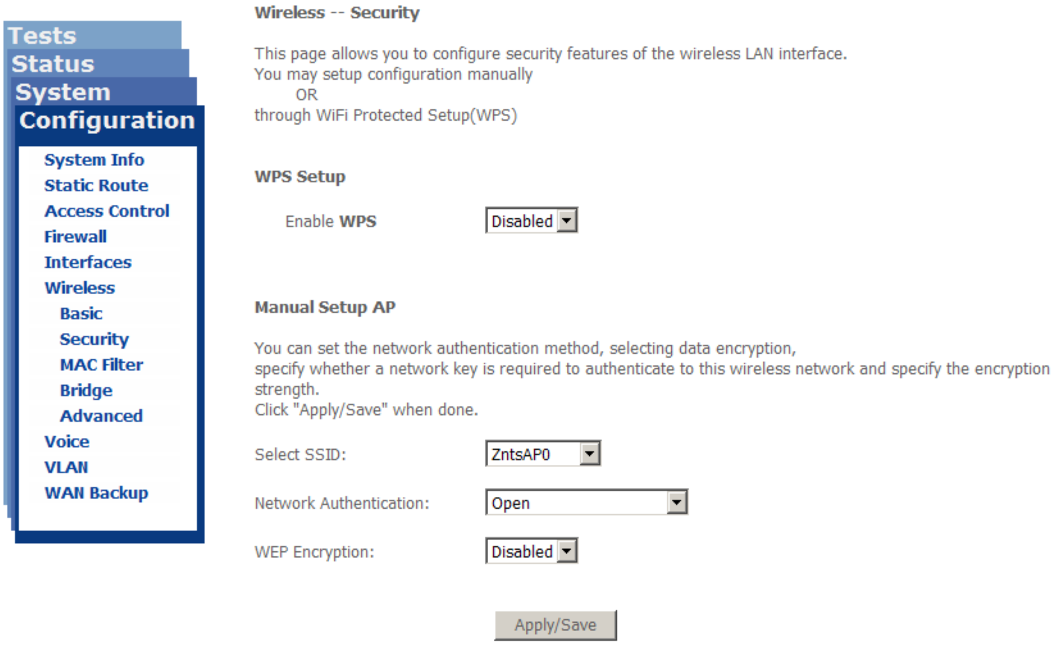
The main items for wireless security are authentication and encryption. Authentication methods which are secure allow the clients (also called stations or STA) you want onto the network, while keeping others off of the network. Encryption is used, both in some of the authentication methods and in the regular transmission of data once the client has successfully completed the authentication process.

Figure 80: Some WiFi authentication and encryption examples


Open (no WPS or WEP encryp)
client (STA)
request sent to AP (clear)
AP authenticates (clear)
STA connects to network (clear)
all future communication for this session is clear
Access Point (AP)
Open (WPS push button. no WEP encryp)
client (STA)
Push virtual button on STA
Push WPS button on rear of AP
AP authenticates
STA connects to network (clear)
all future communication for this session is clear
Access Point (AP)
Shared
client (STA)
request sent to AP (clear)
AP sends challenge (clear)
responds to challenge (encrypted)
if decrypted response matches, AP authenticates STA (encrypted)
STA connects to network (encrypted)
all future communication for this session is encrypted
Access Point (AP)

Wireless security basic options, Table 40 on page 111 describes an overview of the security method and pointers to more detailed information for each security option. Network Authentication parameters (part 1), Table 41 on page 113 and Network Authentication parameters (part 2), Table 42 on page 113 provide a matrix showing the options for each type of authentication and encryption.

Figure 81: The wireless security page



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS: Disabled

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: ZntsAP0

Network Authentication: Open

WEP Encryption: Disabled

Table 40: Wireless security basic options

UI Label	Description
Enable WPS	With **WPA-PSK**, **WPA2-PSK**, **Mixed WPA2/WPA-PSK**, or **Open Network Authentication** modes, there is the ability to add clients via push button or by a STA PIN or AP device PIN. See WPS, page 123
Select SSID	Selects the SSID to associate with the **Network Authorization** mode.

Table 40: Wireless security basic options

UI Label	Description
Network Authentication	• Open Open access to the network. Anyone can access. See Open, page 114. • Shared WEP encryption strength may be 64 or 128 bit. Up to four different keys can be set, though only one it active at any time. See Shared, page 115. • 802.1x An IEEE standard which designed for enterprise use which has an authentication server. See 802.1x, page 116. • WPA WPA strengthens authentication and implements most of the IEEE 802.11i standard, notably adding TKIP encryption. See WPA, page 117. • WPA-PSK WPA-PSK is for small offices and home offices and is mainly WPA without the authentication server. PSK is sometimes referred to the “personal edition” rather than the “enterprise edition.” See WPA-PSK, page 118. • WPA2 WPA2 is an upgrade to WPA whose main enhancement is AES encryption, though AES has since been added to WPA. See WPA2, page 119. • WPA2-PSK WPA2-PSK is enabled by default. WPA2-PSK, like WPA, is mainly WPA2 without the authentication server. See WPA2-PSK, page 120. • Mixed WPA2/WPA Mixed WPA2/WPA supports both WPA2 and WPA in the same environment, and is useful when upgrading between the two authentication methods. See Mixed WPA2/WPA, page 121. • Mixed WPA2/WPA-PSK Like Mixed WPA2/WPA, Mixed WPA2/WPA-PSK supports both WPA2 and WPA-PSK in the same environment, and is the personal edition. Mixed WPA2/WPA-PSK is useful when upgrading between the two authentication methods. See Mixed WPA2/WPA-PSK, page 122.

Table 41: Network Authentication parameters (part 1)

	Open	Shared	802.1x	WPA	WPA-PSK
WEP Encryption	X	X	X	X	X
Encryption Strength		X	X		
Current Network Key		X	X		
Network Key 1		X	X		
Network Key 2		X	X		
Network Key 3		X	X		
Network Key 4		X	X		
RADIUS Server IP Address			X	X	
RADIUS Port			X	X	
RADIUS Key			X	X	
WPA Group Rekey Interval				X	X
WPA/WAPI Passphrase				X	X
WPA/WAPI Encryption					X

Table 42: Network Authentication parameters (part 2)

	WPA2	WPA2-PSK	Mixed WPA2/WPA	Mixed WPA2/WPA-PSK
WEP Encryption		X		X
Encryption Strength				
Current Network Key				
Network Key 1				
Network Key 2				
Network Key 3				
Network Key 4				
RADIUS Server IP Address	X		X	
RADIUS Port	X		X	
RADIUS Key	X		X	
WPA Group Rekey Interval	X	X	X	X

Table 42: Network Authentication parameters (part 2)

	WPA2	WPA2-PSK	Mixed WPA2/WPA	Mixed WPA2/WPA-PSK
WPA/WAPI Passphrase		X		X
WPA/WAPI Encryption	X	X	X	X
WPA2 Preauthentication	X		X	
Network Re-auth Interval	X		X	

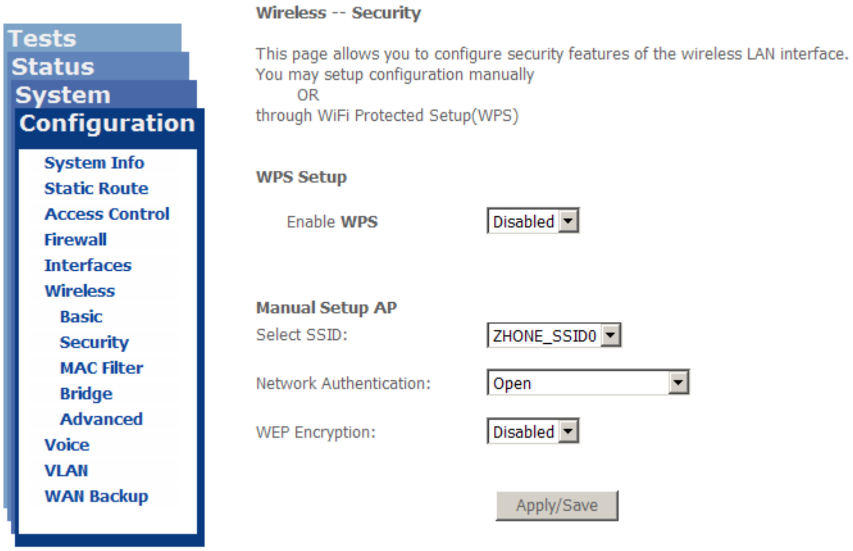
Open

With Network Authentication open and no authentication, anyone can access the network. With WEP Encryption disabled, communication is sent in clear text, so this configuration has no security protection. WiFi Protected Setup (WPS) can be added as an easy yet secure authentication process. WEP encryption can also be added to provide secure communication between the wireless access point (AP) and the clients.

See

- WPS, page 123 for information about WPS setup
- WEP Encryption, page 124 for information about WEP Encryption setup

Figure 82: Wireless security with Open network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS** Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

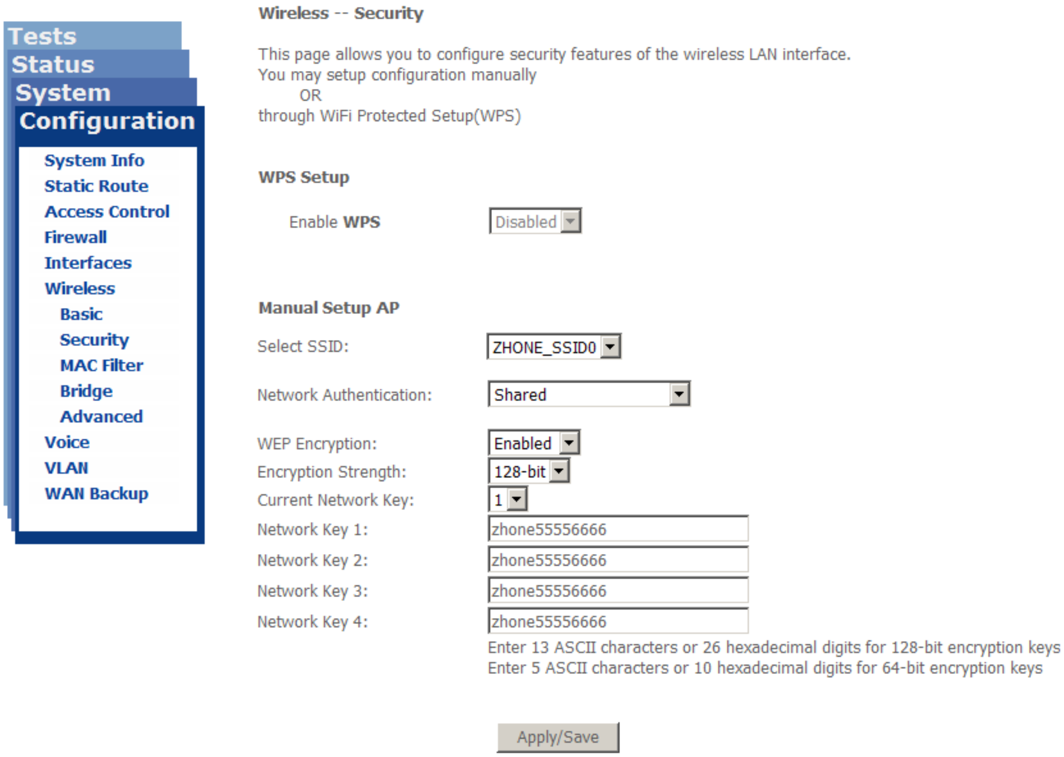
Network Authentication: Open

WEP Encryption: Disabled

Shared

Shared network authentication uses WEP encryption that must be shared between the AP and the STA. The initial request from the STA is in clear text, as is the challenge from the AP. The STA replies to the challenge with the Network Key in an encrypted message.

Figure 83: Wireless security with Shared network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: Shared

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1: zhone55556666

Network Key 2: zhone55556666

Network Key 3: zhone55556666

Network Key 4: zhone55556666

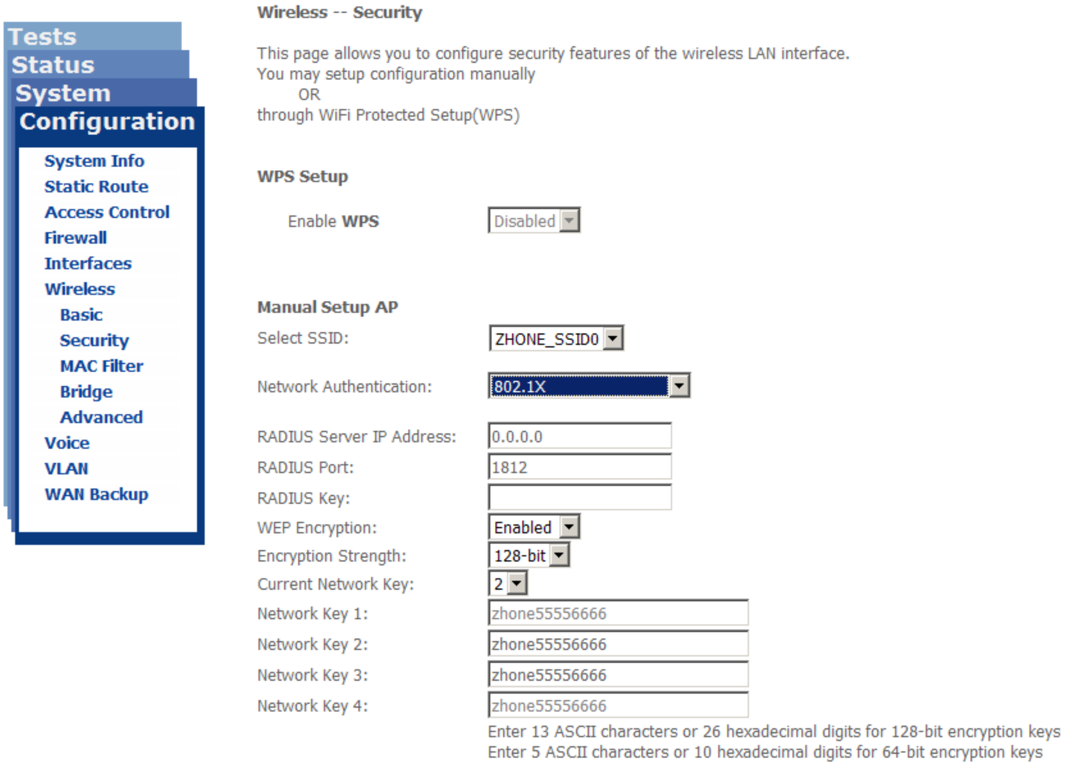
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

802.1x

802.1X network requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is enabled by default with default encryption strength and network keys.

See RADIUS authentication, page 125.

Figure 84: Wireless security with WPA network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1: zhone55556666

Network Key 2: zhone55556666

Network Key 3: zhone55556666

Network Key 4: zhone55556666

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

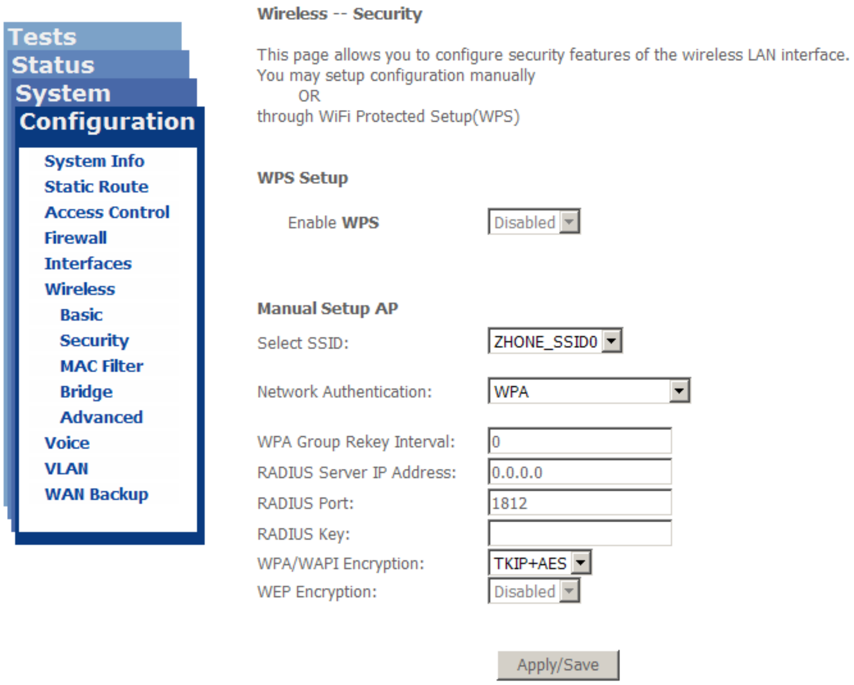
WPA

WPA (WiFi Protected Access) is usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP+AES uses 128-bit dynamic session keys (per user, per session, and per packet keys). Dynamically creating a new key for each packet prevents collisions.

AES (Advanced Encryption Standard) is stronger than TKIP. However, the options provided by the zNID 24xx are TKIP+AES and AES. AES is a later addition to WPA.

Network re-authorization interval is the time in which another key needs to be dynamically issued.

Figure 85: Wireless security with WPA network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

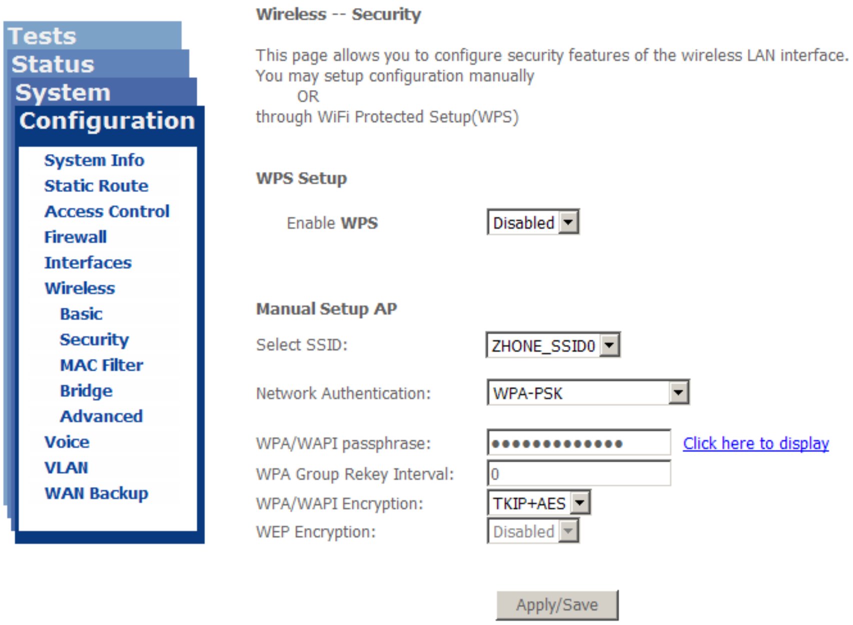
WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

WPA-PSK

WPA-PSK (WiFi Protected Access – Pre-Shared Key) is basically WPA for home and small office/home office (SOHO) environments. WPA-PSK uses the same strong TKIP+AES encryption which is used for WPA, per-packet key construction, and key management that WPA provides in the enterprise environment. However unlike WPA which uses a RADIUS server, WPA-PSK uses a password (WPA/WAPI passphrase) which is entered manually. A group re-key interval time is also required.

Figure 86: Wireless security with WPA-PSK network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: WPA-PSK

WPA/WAPI passphrase: ●●●●●●●●●●●●● Click here to display

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: TKIP+AES

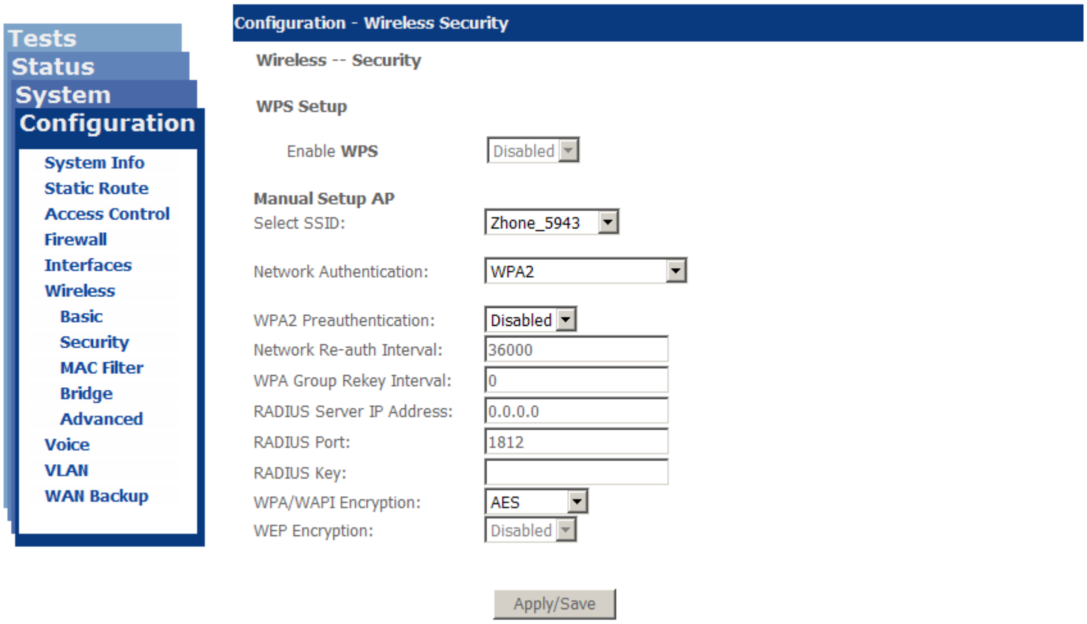
WEP Encryption: Disabled

WPA2

WPA2 (WiFi Protected Access 2) — second generation WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method.

Network re-authorization interval is the time in which another key needs to be dynamically issued.

Figure 87: Wireless security with WPA2 network authentication



Configuration - Wireless Security

Wireless -- Security

WPS Setup

Enable WPS	Disabled

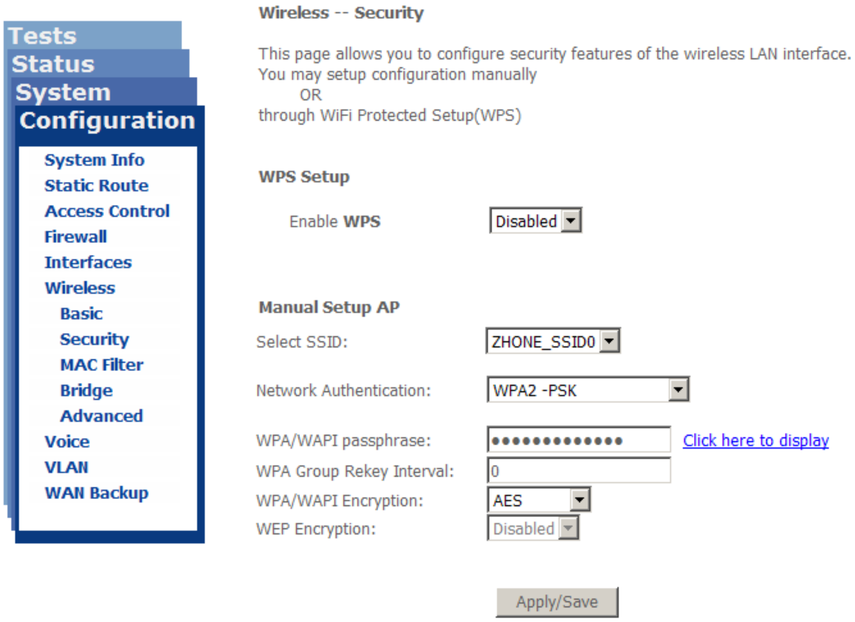
Manual Setup AP

Select SSID:	Zhone_5943
Network Authentication:	WPA2
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

WPA2-PSK

WPA2-PSK (WiFi Protected Access 2 – Pre-Shared Key) — suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and a re-key interval time.

Figure 88: Wireless security with WPA2-PSK network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ●●●●●●●●●●●●● Click here to display

WPA Group Rekey Interval: 0

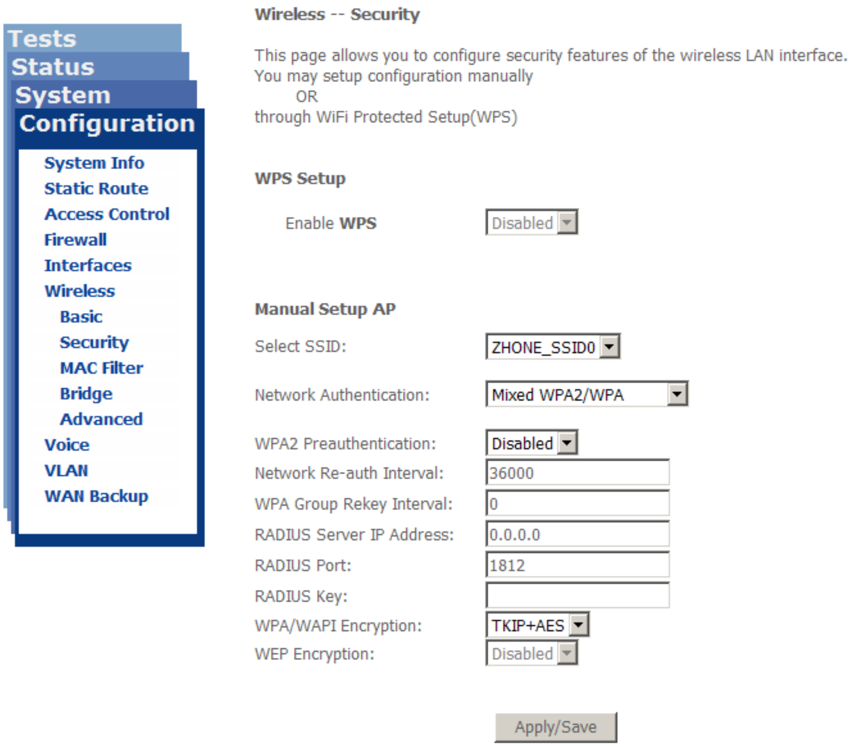
WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Mixed WPA2/WPA

Mixed WPA2 / WPA — useful during transitional times for upgrades in the enterprise environment, this mixed authentication method allows "upgraded" and users not yet "upgraded" to access the network via the router. RADIUS server information must be entered for WPA and a as well as a group re-key interval time. Both TKIP and AES are used.

Figure 89: Wireless security with Mixed WPA2/WPA network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: Mixed WPA2/WPA

WPA2 Preauthentication: Disabled

Network Re-auth Interval: 36000

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

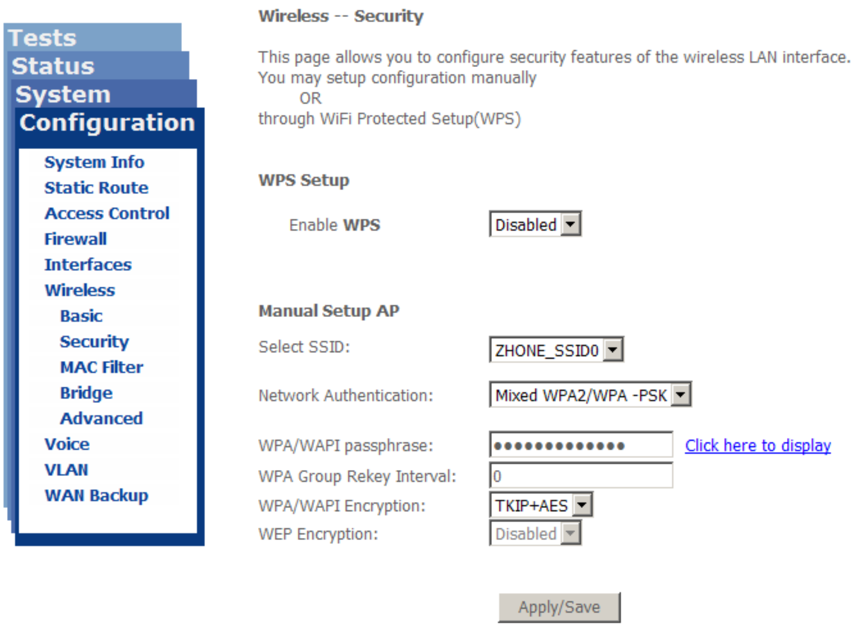
WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

Mixed WPA2/WPA-PSK

Mixed WPA2 / WPA-PSK — useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.

Figure 90: Wireless security with Mixed WPA2/WPA-PSK network authentication



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

Select SSID: ZHONE_SSID0

Network Authentication: Mixed WPA2/WPA -PSK

WPA/WAPI passphrase: ●●●●●●●●●●●●● Click here to display

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

WPS

With WiFi Protected Setup (WPS) — available for WPA-PSK, WPA2-PSK, Mixed WPA2/WPA-PSK and Open Network Authentication methods — the wireless zNID 24xx can add clients via three different methods:

- push button certification

  With push button certification you must simultaneously push the WPS button on the rear panel of the wireless zNID 24xx and click the virtual button for push button registration on the client device.

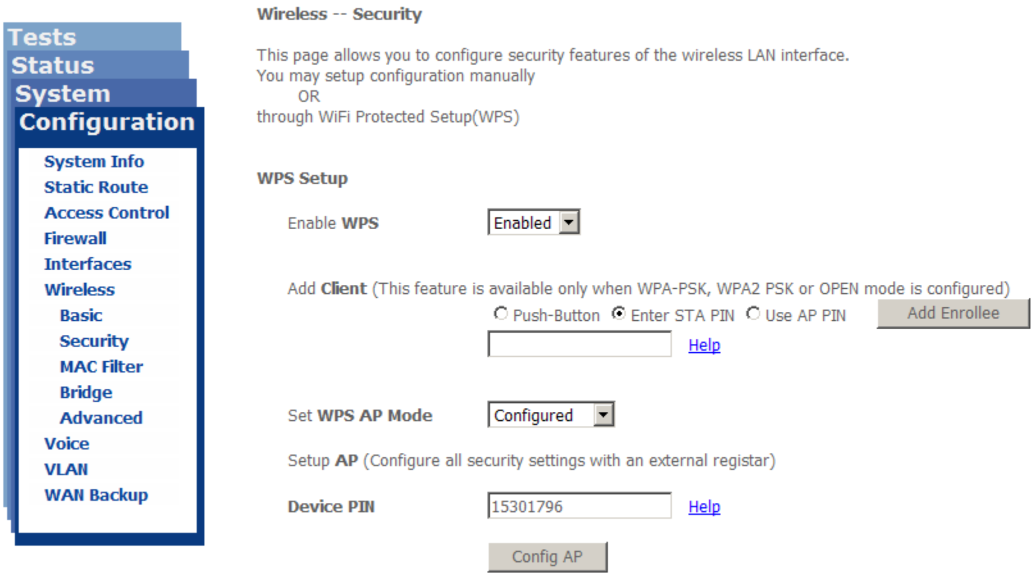
- entering the STA PIN

  For STA PIN, a personal identification number (PIN) which matches the PIN from the wireless network client (also called station) is entered into the text box beneath the WPS add client radio buttons. Unlike most situations where the server provides the password, in this situation the client provides the password and the AP acknowledges it.

- entering the AP PIN

  For AP setup, a device PIN is entered in the Device PIN text box. The clients must match the device PIN to access.

Figure 91: WPS configuration



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable **WPS** Enabled

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
○ Push-Button ● Enter STA PIN ○ Use AP PIN Add Enrollee
Help

Set **WPS AP Mode** Configured

Setup **AP** (Configure all security settings with an external registar)

Device PIN 15301796 Help

Config AP

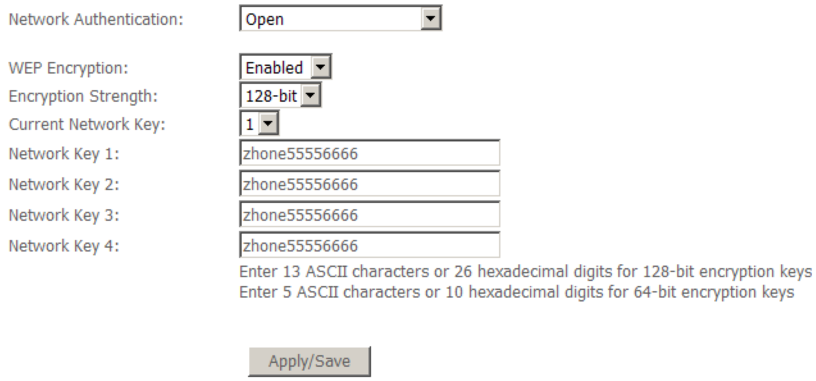
Set WPS AP Mode

If your provider is using an external registrar for security, select Configured. The PIN for AP mode is specified by the registrar. Provide this PIN to the client. Click **Config AP** to begin the registration process with the client.

WEP Encryption

WEP (Wire Equivalent Privacy) is encryption based on an encryption key strength of 64 or 128 bits. Up to 4 different keys can be set and you can come back to select which one to use at anytime.

Figure 92: Setting up WEP network keys



Network Authentication: Open

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1: zhone55556666

Network Key 2: zhone55556666

Network Key 3: zhone55556666

Network Key 4: zhone55556666

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Table 43: Configuration parameters for WEP Encryption Enabled

UI Label	Description
WEP Encryption	Enabled has WEP encryption on, disabled is clear text (NOTE that some authentication methods use WEP Encryption by default so the WEP Encryption dropdown will only allow Enabled. Other authentication methods which do not use WEP encryption will only allow Disabled and be grayed out.)
Encryption Strength	64 or 128 bits. For 64 bit encryption 10 hexadecimal digits or 5 ASCII characters are entered. For 128 bit encryption 26 hexadecimal digits or 13 ASCII characters are entered. The network key is concatenated with an initialization vector to form an RC4 key.
Current Network Key	Allows you to select one of the four Network keys.
Network Key 1, 2, 3, 4	Provide the network key input for the RC4 key.

RADIUS authentication

Remote Access Dial-Up Service (RADIUS) is not only for WiFi applications. The RADIUS server requires identity and credentials (username and password) from the user and is used for enterprise security.

Figure 93: RADIUS authentication uses an authentication server

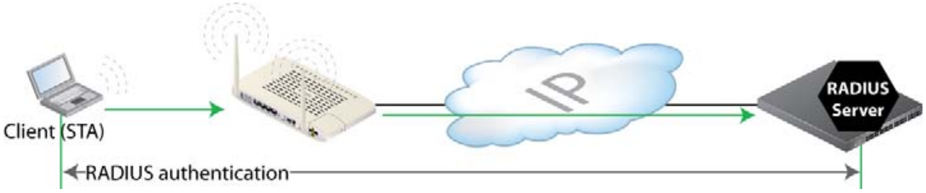


Table 44: RADIUS authentication parameters

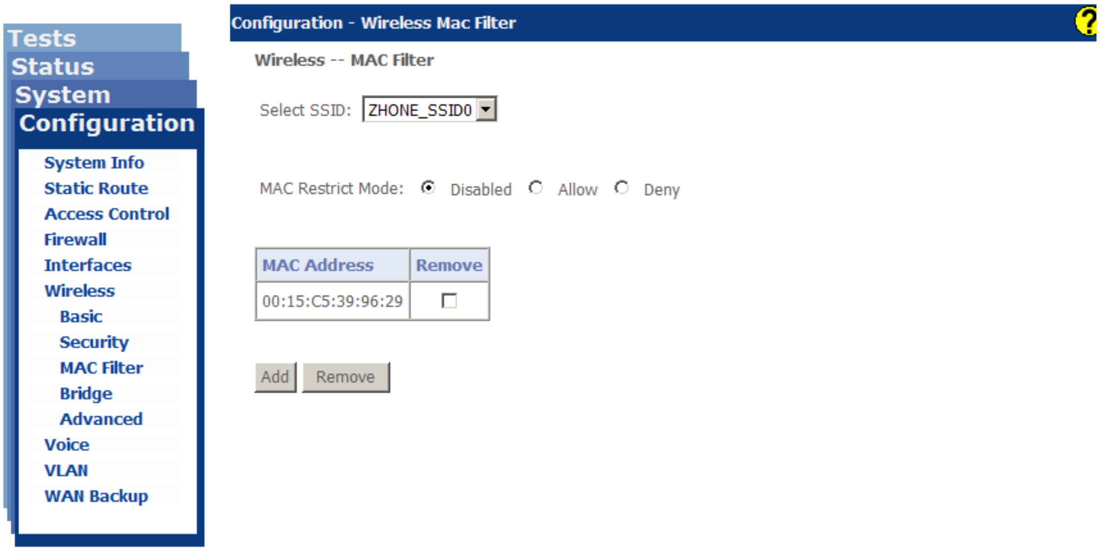
UI Label	Description
RADIUS Server IP Address	IP address of the RADIUS server
RADIUS Port	Port which the authentication application is using on the RADIUS server
RADIUS Key	Key which is being used to authenticate the zNID 24xx with the RADIUS server

MAC filter

To restrict wireless access to an AP by SSID, you can add a MAC Filter which filters for the MAC address. The filter defines whether a client can connect to the AP based on the MAC address of the client.

The list of MAC addresses can allow a list of devices to use the AP or the list can be denied use.

Figure 94: The MAC filter page with no MAC addresses entered



Configuration - Wireless Mac Filter

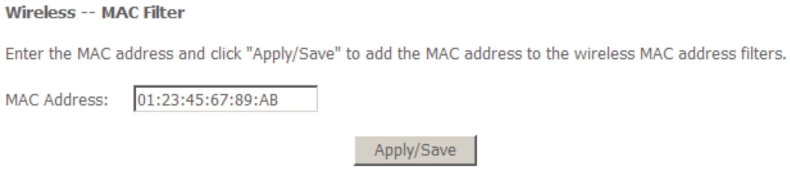
Wireless -- MAC Filter

Select SSID: ZHONE_SSID0

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove
00:15:C5:39:96:29	□

Figure 95: Add a MAC address for a wireless client

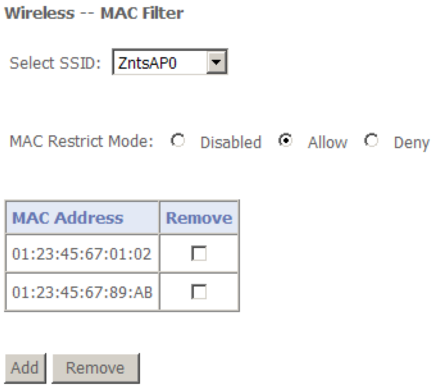


Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address: 01:23:45:67:89:AB

Figure 96: The MAC filter list can allow or deny a group of devices



Wireless -- MAC Filter

Select SSID: ZntsAP0

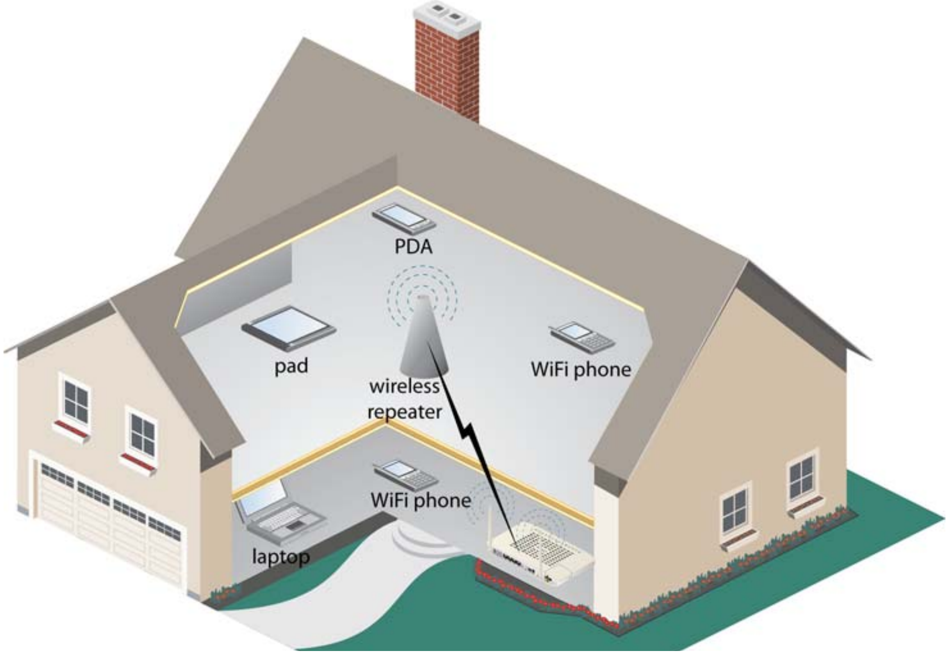
MAC Restrict Mode: ○ Disabled ● Allow ○ Deny

MAC Address	Remove
01:23:45:67:01:02	□
01:23:45:67:89:AB	□

Wireless bridge

The **Wireless Bridge** page allows you to configure wireless bridge (also known as Wireless Distribution System (WDS)) functionality. WDS allows for the expansion of the wireless network across multiple access points without wired connections. Wireless bridge refers to the connection between the AP and a wireless repeater device which extends the reach of the AP.

Figure 97: A common scenario for a wireless bridge



A key to setting up the wireless repeater is to use the same SSID and login credentials.

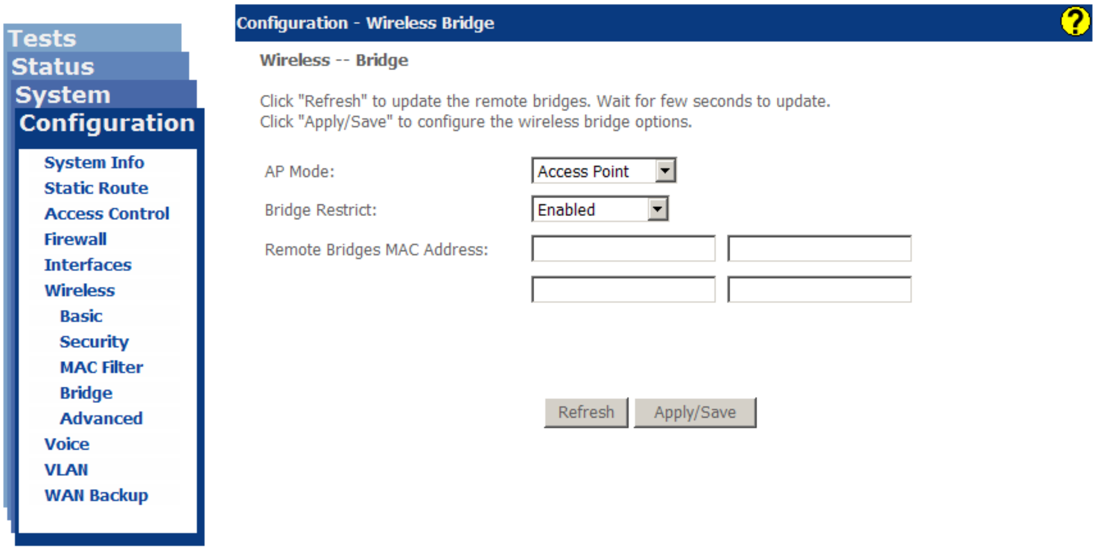
Table 45: WDS parameters

UI Label	Description
AP Mode	• **Access Point** Both AP and WDS are enabled • **Wireless Bridge** Only WDS is enabled, otherwise the AP is disabled

Table 45: WDS parameters

UI Label	Description
Bridge Restrict	Applies to the wireless bridge: • **Enabled** Access is restricted to devices whose MAC addresses are entered in the text boxes for **Remote Bridge MAC Address** • **Enabled(Scan)** Scans for any wireless bridge devices in range and displays them in the **Remote Bridge MAC Address** table. Select the wireless bridge device via the checkbox. Clicking Refresh will update the wireless bridge devices in range. Wait for a few seconds for the update. • **Disabled** Any wireless bridge device will be granted access.

Figure 98: Wireless bridge page with Bridge Restrict set to Enabled



Configuration - Wireless Bridge

Wireless -- Bridge

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode: Access Point

Bridge Restrict: Enabled

Remote Bridges MAC Address:

Table 46: Wireless Distribution System options

UI Label	Description
AP Mode	Defines the WDS modes • **Access Point** Sets the wireless network for AP and WDS functionality • **Wireless Bridge** Sets the wireless network for WDS functionality only

Table 46: Wireless Distribution System options

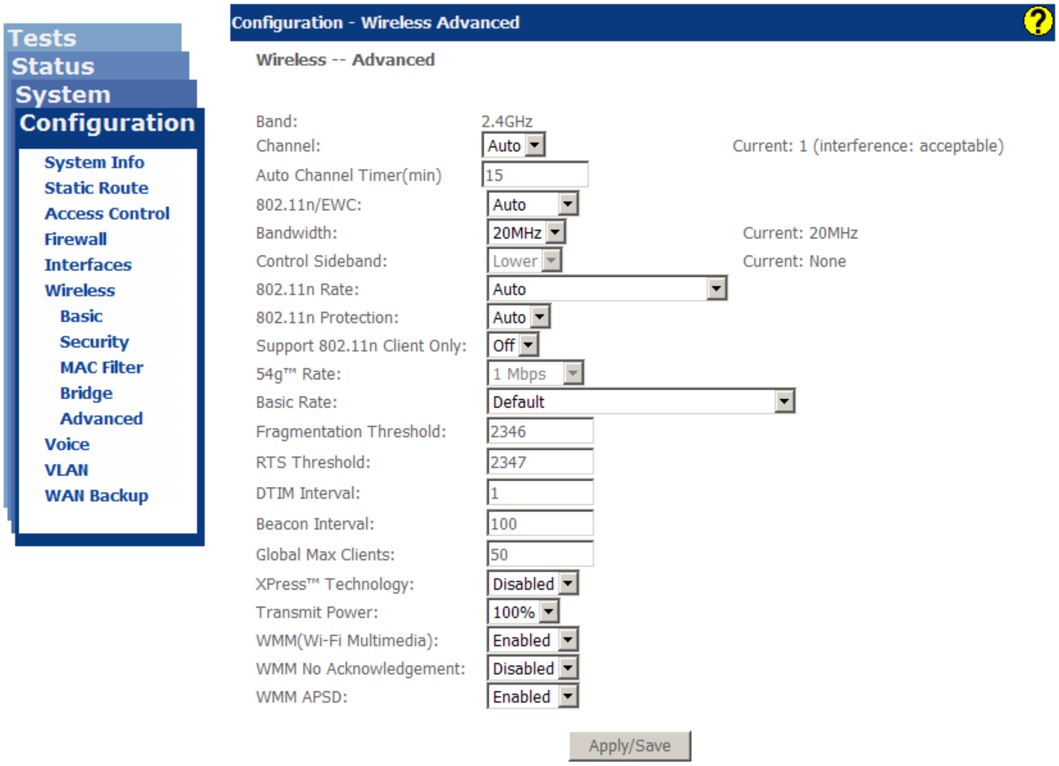
UI Label	Description
Bridge Restrict	Defines the access for wireless bridge devices • **Enabled** Allows only the devices with MAC addresses entered in the **Remote Bridges MAC Address** text boxes (up to four) • **Enabled(Scan)** Scans for wireless devices in range and enters them in a list. Normally items without an SSID entered are client devices. Devices with an SSID are wireless AP and possibly could be a WDS network extender • **Disabled** Allows any wireless bridge access

Advanced

The **Wireless | Advanced** page configure wireless signal settings.

Note: Do not change the settings on this page if you are not familiar with WiFi settings.

Figure 99: Advanced wireless signal setting parameters



Configuration - Wireless Advanced

Wireless -- Advanced

Band: 2.4GHz
Channel: Auto — Current: 1 (interference: acceptable)
Auto Channel Timer(min): 15
802.11n/EWC: Auto
Bandwidth: 20MHz — Current: 20MHz
Control Sideband: Lower — Current: None
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
54g™ Rate: 1 Mbps
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 50
XPress™ Technology: Disabled
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled
WMM No Acknowledgement: Disabled
WMM APSD: Enabled

Table 47: Advanced wireless settings

UI Label	Description
Band	2.4GHz – 802.11g
Channel	Defines which channel to use. 802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your zNID. Auto automatically selects a channel with low interference.

Table 47: Advanced wireless settings

UI Label	Description
Auto Channel Timer(min)	Defines the refresh time in minutes for rescans which finds the best available channel for use on your wireless network. When configured for auto mode, the timer value specifies how often to re-analyze the spectrum to select a low interference channel. Note: auto channel rescan will only occur when there are no actively connected devices.
802.11n/EWC	Not currently used. • Auto Enables 802.11n/EWC bandwidth • Disabled Disables 802.11n/EWC bandwidth
Bandwidth	Bandwidth of the 802.11n/EWC configuration, either 20MHz or 40MHz. 802.11n/EWC must be selected.
Control Sideband	Selects the control sideband when Bandwidth of 40MHz is selected. 802.11n/EWC must be set to Auto.
802.11n Rate	The transfer rate from the zNID to the wireless client. When **Auto** is selected the zNID uses the fastest mutually support rate which can be used with the current signal strength and noise levels. Fixed rates limit the maximum rate to the specified value. **Auto** is the recommended setting.
802.11n Protection	802.11n protection is a physical level protection which allows 802.11n devices to transmit a Clear-to-send (CTS) frame to itself to ensure that the neighboring legacy devices will use the timing information to protect 802.11n frames which follow. **Auto** is the recommended setting.
Support 802.11n Client Only	802.11n only mode is enabled to prevent low speed clients (such as 802.11b) from wasting time with low speed transmissions. WiFi is a time division duplexed technology, meaning that it is a half duplex ping-pong type scheme. The system capacity goes WAY DOWN when a low speed client is connected. • **On:** Prevents 802.11b/g clients from connecting • **Off:** Allows 802.,11b/g clients as well as 802.11n clients
RIFS Advertisement	RIFS (Reduced Inter-Frame Spacing) reduces the amount of time (unused time) between Orthogonal Frequency-Division Multiplexing (ODFM) transmission to improve performance. 802.11n/EWC must be selected.

Table 47: Advanced wireless settings

UI Label	Description
54g™ Rate	The rate at which information will be transmitted and received on your wireless network.
Multicast Rate	Multicast rate is the transmission rate for multicast packets. Since multicast packets are sent once and must be received by all clients, they must be sent at a low enough rate for all clients to receive. Fixed rate specifies a fixed rate to always be used for multicast transmissions. **Auto** mode uses the rate of the lowest speed client that is currently connected.
Basic Rate	The set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium. The default setting (Default) transmits at all standard wireless rates (1-2Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, and 24 Mbps).
Fragmentation Threshold	used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
RTS Threshold	determines the packet size of a transmission through the use of the router to help control traffic flow.
DTIM Interval	sets the Wake-up interval for clients in power-saving mode.
Beacon Interval	a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
Global Max Clients	Sets the maximum limit on the total number of client which can connect to the AP. **Global Max Clients** is the sum of all clients connected to all SSIDs. The **Max Clients** parameter in the **Wireless | Basic** page sets the maximum number of clients per the selected or named SSID. The sum of all **Max Clients** per SSID must be less than or equal to the **Global Max Clients** value.
XPress™ Technology	a technology that utilizes standards based on frame bursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b equipment.
Transmit Power	Select from 20%, 40%, 60%, 80% and 100%. The default value is 100%.

Table 47: Advanced wireless settings

UI Label	Description
WMM (WiFi Multimedia)	prioritizes traffic from different applications such as voice, audio and video applications under different environments and conditions.
WMM No Acknowledgement	the acknowledgement policy used on the MAC level. Enabling no-acknowledgement can result in efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	APSD (Automatic Power Save Delivery). APSD manages radio usage for battery-powered devices to allow battery life in certain conditions. APSD allows a longer beacon interval until an application—VoIP for example — requiring a short packet exchange interval starts. Only if the wireless client supports APSD does APSD affect radio usage and battery life.

Voice

The zNIDs support SIP, SIP-PLAR and MGCP protocols.

- *SIP* on page 135
- *SIP-PLAR* on page 136
- *MGCP* on page 139

SIP and SIP-PLAR have many of the same parameters as can be seen in Figure 101, SIP configuration, Figure 103, SIP-PLAR configuration and.Table 48. See Table 48 for both SIP and SIP-PLAR parameters.

SIP

The SIP configuration connects via network to a SIP softswitch.

Figure 100: SIP scenario

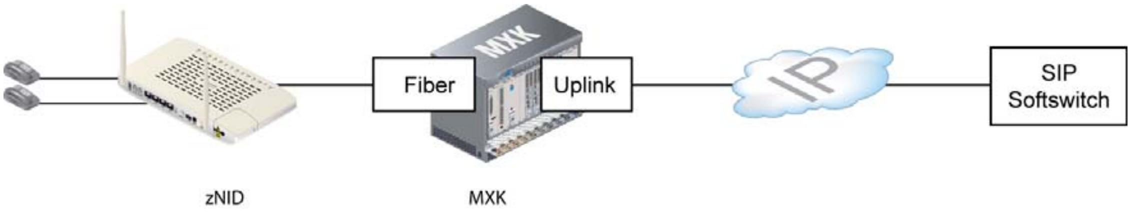
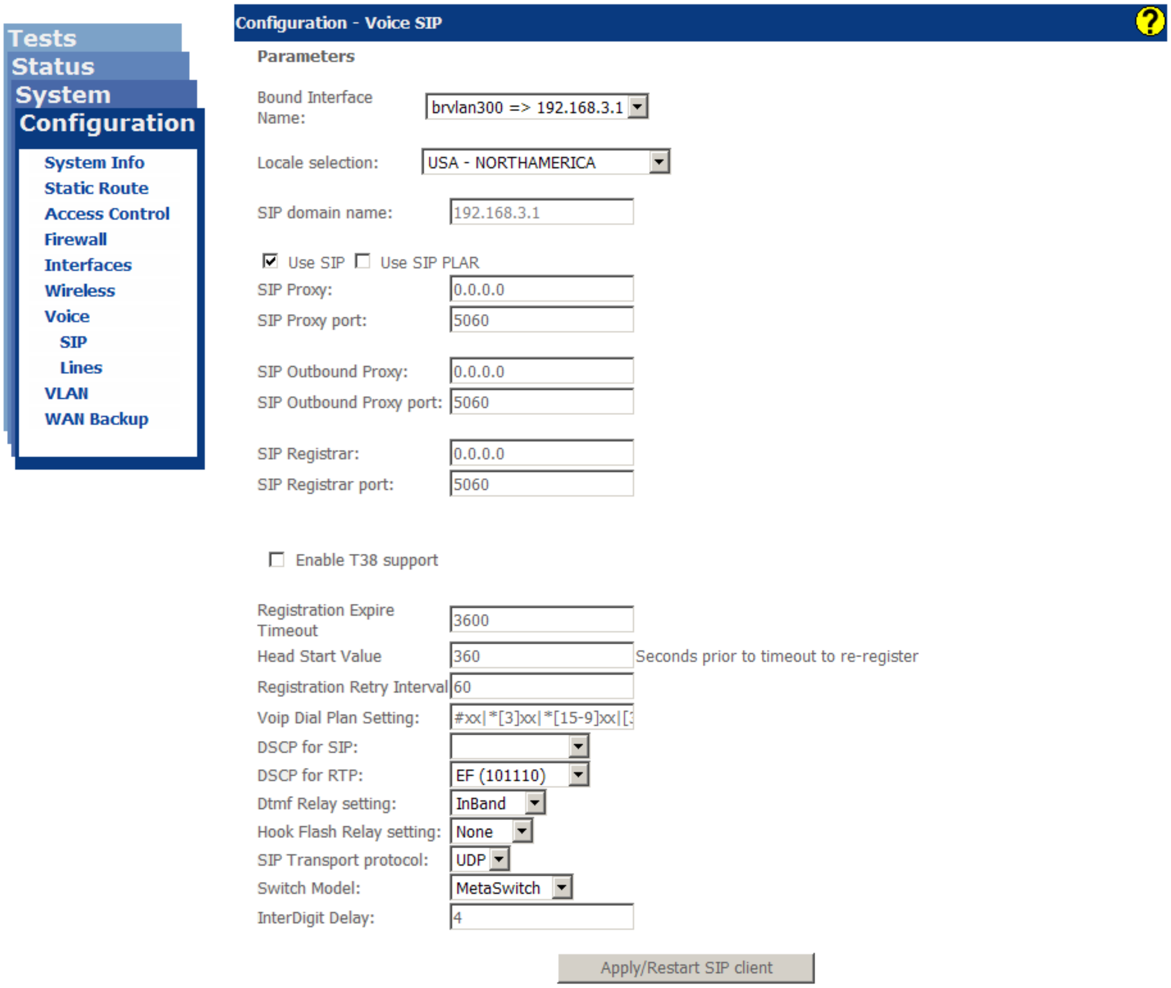


Figure 101: SIP configuration



Configuration - Voice SIP

Parameters

Bound Interface Name:	brvlan300 => 192.168.3.1
Locale selection:	USA - NORTHAMERICA
SIP domain name:	192.168.3.1
☑ Use SIP ☐ Use SIP PLAR	
SIP Proxy:	0.0.0.0
SIP Proxy port:	5060
SIP Outbound Proxy:	0.0.0.0
SIP Outbound Proxy port:	5060
SIP Registrar:	0.0.0.0
SIP Registrar port:	5060
☐ Enable T38 support	
Registration Expire Timeout	3600
Head Start Value	360 Seconds prior to timeout to re-register
Registration Retry Interval	60
Voip Dial Plan Setting:	#xx|*[3]xx|*[15-9]xx|[
DSCP for SIP:	
DSCP for RTP:	EF (101110)
Dtmf Relay setting:	InBand
Hook Flash Relay setting:	None
SIP Transport protocol:	UDP
Switch Model:	MetaSwitch
InterDigit Delay:	4

Define the changes to the configuration and click **Apply/Restart SIP client**, The SIP client will be restarted. Existing phone calls will be terminated.

SIP-PLAR

The Zhone SIP-PLAR implementation has a voice gateway which connects to the Class V switch.

Figure 102: SIP-PLAR scenario

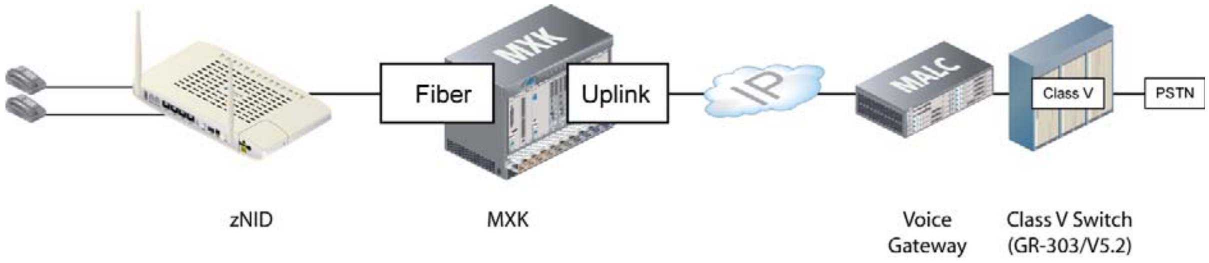
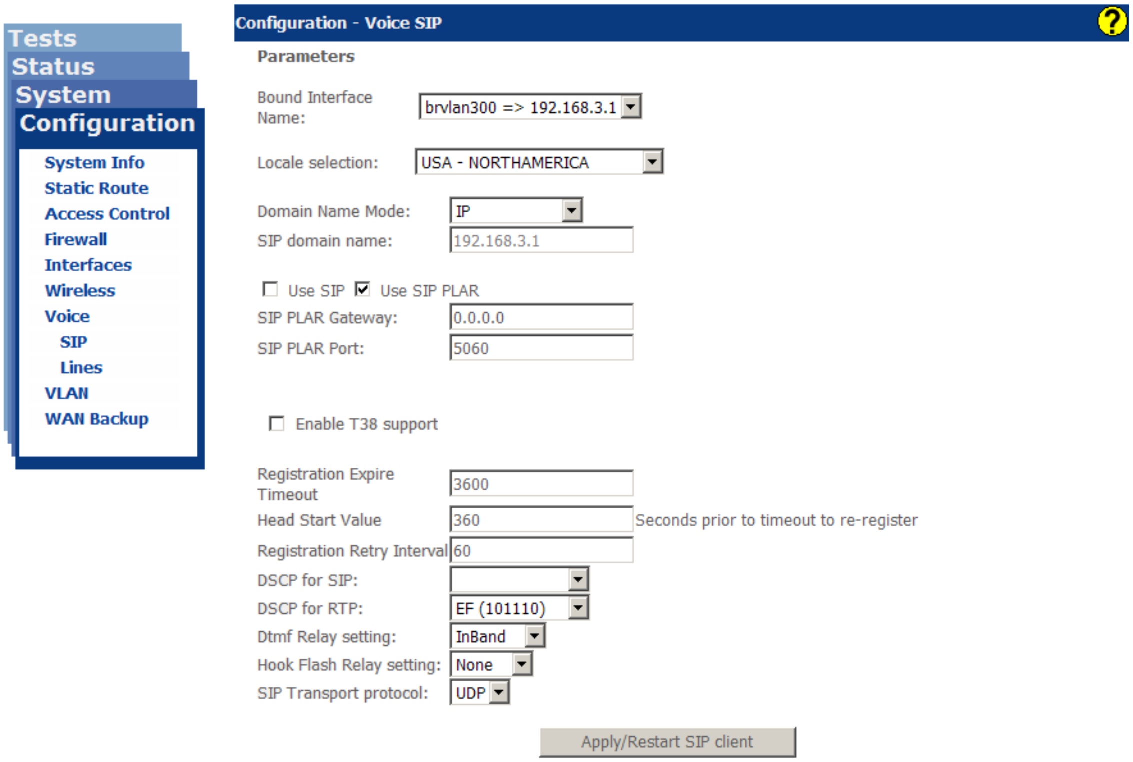


Figure 103: SIP-PLAR configuration



Configuration - Voice SIP

Parameters

Bound Interface Name:	brvlan300 => 192.168.3.1
Locale selection:	USA - NORTHAMERICA
Domain Name Mode:	IP
SIP domain name:	192.168.3.1

□ Use SIP ☑ Use SIP PLAR

SIP PLAR Gateway:	0.0.0.0
SIP PLAR Port:	5060

□ Enable T38 support

Registration Expire Timeout	3600
Head Start Value	360 Seconds prior to timeout to re-register
Registration Retry Interval	60
DSCP for SIP:	
DSCP for RTP:	EF (101110)
Dtmf Relay setting:	InBand
Hook Flash Relay setting:	None
SIP Transport protocol:	UDP

Define the changes to the configuration and click Apply/Restart SIP client, The SIP client will be restarted. Existing phone calls will be terminated.

Table 48: SIP and SIP-PLAR configuration

UI Label	Description
Bound Interface Name:	A list displaying all the interfaces in the box which have been assigned an IP address. Select the Interface for the switch to address with the changes from this page.

Table 48: SIP and SIP-PLAR configuration

UI Label	Description
Locale Selection:	Select the country. This field sets the phone to respond as expect in the selected country.
Domain Name Mode	**SIP Mode only** Defines whether an IP address or a domain name will be used to identify the SIP domain.
SIP domain name	The information you add in the **SIP domain name** depends on the selection for the **Domain Name Mod**e dropdown. The IP address or the domain name for the VoIP client.
SIP or SIP-PLAR checkboxes	Select SIP or SIP PLAR. Note that the selection adjusts the screen to the items that are needed for the protocol.
SIP Proxy:	**SIP Mode Only:** the address of the SIP Proxy Switch.
SIP Proxy port:	**SIP Mode Only:** the port number of the SIP Proxy Switch. Enter 0 to enable DNS SRV mode.
Use SIP Outbound Proxy:	**SIP Mode Only:** the address number of the SIP Outbound Proxy Switch.
SIP Outbound Proxy:	**SIP Mode Only:** the address number of the SIP Outbound Proxy Switch. Enter 0 to enable DNS SRV mode.
SIP Outbound Proxy port:	**SIP Mode Only:** the port of the SIP Outbound Proxy Switch.
SIP Registar:	**SIP Mode Only:** the address number of the SIP registar Switch.
SIP Registar port:	**SIP Mode Only:** the port number of the SIP registar Switch. Enter 0 to enable DNS server mode.
SIP PLAR Gateway	**SIP PLAR Mode Only:** the address number of the SIP PLAR Switch.
SIP PLAR Port	**SIP PLAR Mode Only:** the port number of the SIP PLAR Switch.
Enable T38 support:	Allow T38 FAX on this phone line.
Registration Expire Timeout:	Timeout value for registration process.
Head Start Value	Seconds prior to registration time out to start new registration. If Registration Expire Timeout is 3600 and Head Start Value is 3540 then (3600 - 3540) the router would re-register every minute.
Registration Expire Interval	Time to wait before reissuing a Registration that was not responded to.
Voip Dial Plan Setting	**SIP Mode Only:** Regular Grammar describing valid phone number.

Table 48: SIP and SIP-PLAR configuration

UI Label	Description
DSCP for SIP	Priority Value for protocol data.
DSCP for RTP	Priority Value for voice data.
Dtmf Relay setting	Method of sending tones.
Hook Flash Relay setting	Method of sending Hook transition.
SIP Transport protocol	Send information over UDP or TCP.
Switch Model	SIP Mode Only: Used to configure dial features.
InterDigit Timeout	SIP Mode Only: In Dial plan the T value is a timeout value. This is the duration of the T value.

MGCP

The MGCP configuration connects via network to a MGCP softswitch.

Figure 104: MGCP scenario

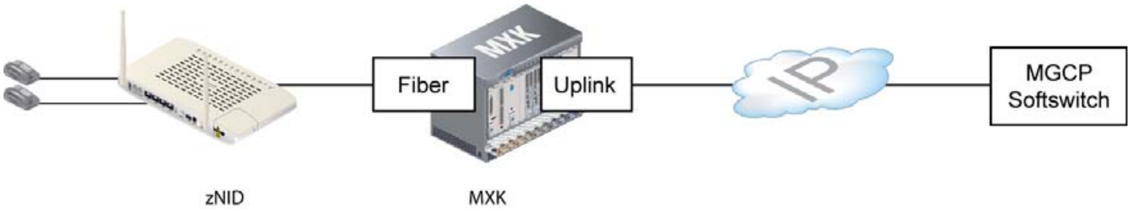
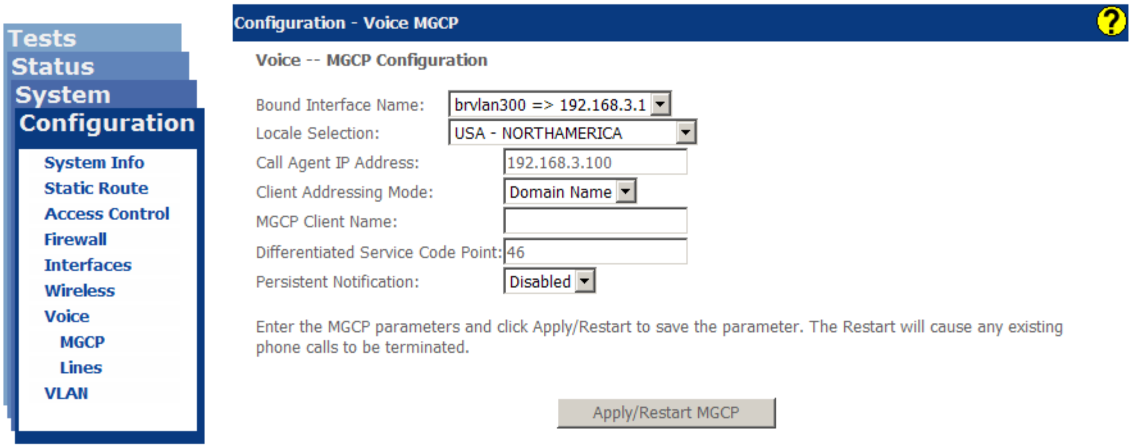


Figure 105: MGCP configuration



Configuration - Voice MGCP

Voice -- MGCP Configuration

Bound Interface Name:	brvlan300 => 192.168.3.1
Locale Selection:	USA - NORTHAMERICA
Call Agent IP Address:	192.168.3.100
Client Addressing Mode:	Domain Name
MGCP Client Name:	
Differentiated Service Code Point:	46
Persistent Notification:	Disabled

Enter the MGCP parameters and click Apply/Restart to save the parameter. The Restart will cause any existing phone calls to be terminated.

Define the changes to the configuration and click Apply/Restart SIP client, The SIP client will be restarted. Existing phone calls will be terminated.

Table 49: MGCP configuration

UI Label	Description
Bound Interface Name	A list displaying all the interfaces in the box which have been assigned an IP address. Select the Interface for the switch to address with the changes from this page.
Locale Selection	Select the country. This field sets the phone to respond as expect in the selected country
Call Agent IP Address	The Address of the MGCP switch.
Client Addressing Mode	IP and Bracketed will cause the MGCP Client name to be the Bound Interface IP address. Name will allow the user to input any text field, usually a Domain Name
MGCP Client Name	The IP address of the VoIP call stack in this ONU
Differentiated Service Code Point	Value of the DSCP which is used to prioritize traffic through the network

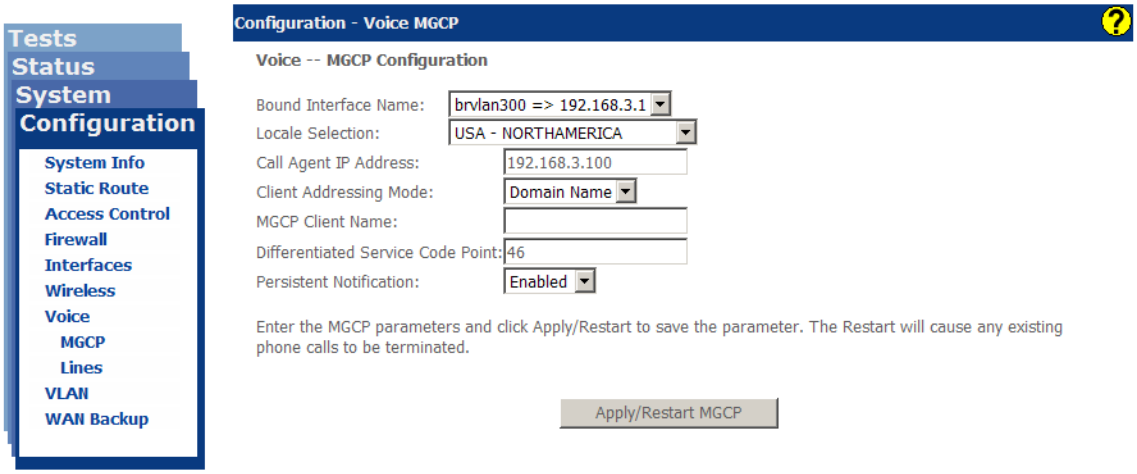
Table 49: MGCP configuration

UI Label	Description
Persistent Notification	When enabled, all switchhook events will be forwarded to the switch immediately without regards to what the switch has requested. When disabled, the event that the switch has requested will be forwarded.

Lines

The **Configuration | Voice | Lines** page selects which physical POTS interfaces are made active as well as setting signal information for the lines.

Figure 106: MGCP Line configuration



Voice -- MGCP Configuration

Bound Interface Name: brvlan300 => 192.168.3.1

Locale Selection: USA - NORTHAMERICA

Call Agent IP Address: 192.168.3.100

Client Addressing Mode: Domain Name

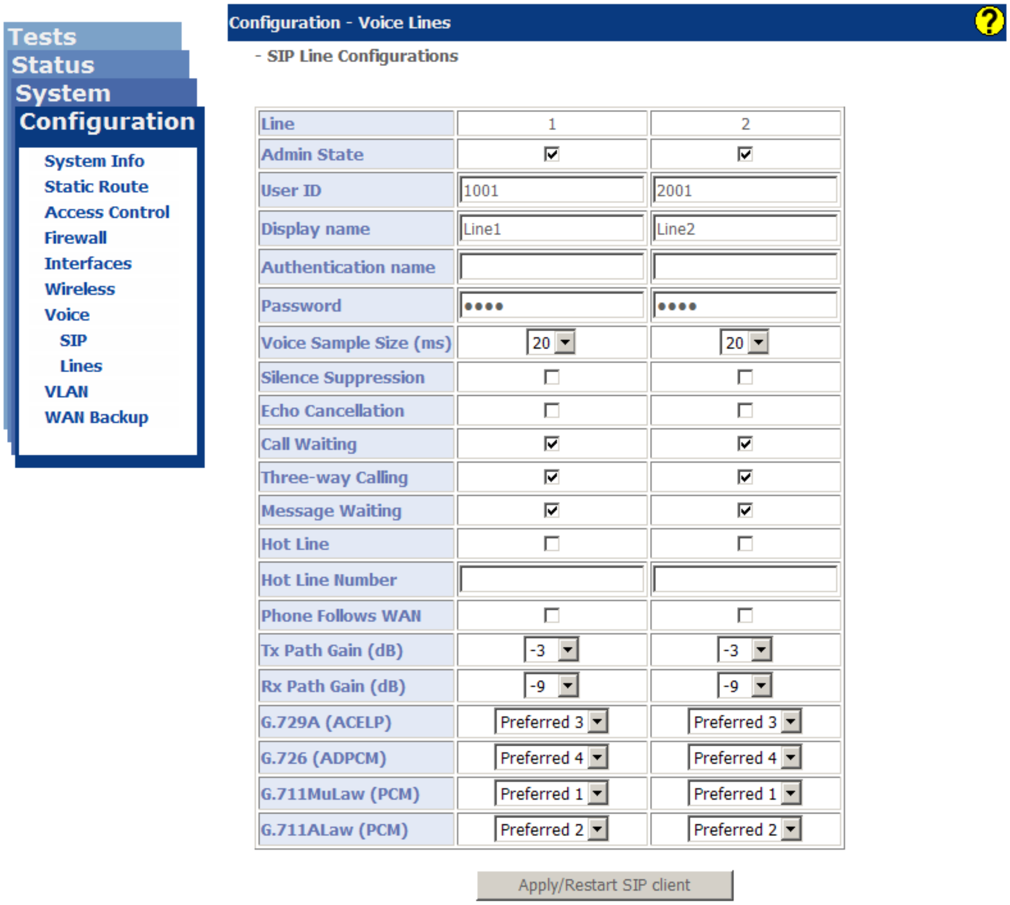
MGCP Client Name:

Differentiated Service Code Point: 46

Persistent Notification: Enabled

Enter the MGCP parameters and click Apply/Restart to save the parameter. The Restart will cause any existing phone calls to be terminated.

Figure 107: SIP Line configuration



Configuration - Voice Lines

- SIP Line Configurations

Line	1	2
Admin State	☑	☑
User ID	1001	2001
Display name	Line1	Line2
Authentication name		
Password	●●●●	●●●●
Voice Sample Size (ms)	20	20
Silence Suppression	□	□
Echo Cancellation	□	□
Call Waiting	☑	☑
Three-way Calling	☑	☑
Message Waiting	☑	☑
Hot Line	□	□
Hot Line Number		
Phone Follows WAN	□	□
Tx Path Gain (dB)	-3	-3
Rx Path Gain (dB)	-9	-9
G.729A (ACELP)	Preferred 3	Preferred 3
G.726 (ADPCM)	Preferred 4	Preferred 4
G.711MuLaw (PCM)	Preferred 1	Preferred 1
G.711ALaw (PCM)	Preferred 2	Preferred 2

Table 50: Voice line configuration

UI Label	Description
Line	The number matches the physical POTS port on the zNID.
Admin State	When checked the port is Enabled to the switch.
User ID	Text Field to allow user to identify the port. The recommended ID is phone number.
Line Name or Display Name	Text Field that identifies the port to the switch. This must match what the Service Provider has set.
Authentication Name	Optional, required by some switches
Password (SIP only)	Security passkey for connecting to the SIP server, assigned by voice service provider
Voice Sample Size (ms)	The time that the DSP will encode voice before sending. The longer the time the more propagation delay in the data stream, but also the more efficient the packetization.

Table 50: Voice line configuration

UI Label	Description
Silence Suppression	Check enables Silence Suppression.
Echo Cancellation	Check enables Echo Cancellation.
Call Waiting	Check enables Call Waiting
Three-way Calling	Check enables Three-way calling
Message Waiting	When enabled, a SUBSCRIBE message will be sent after Registration to subscribe to message waiting.
Hotline Enable	When enabled the phone will immediately dial the Hotline number.
Hotline Number	The only number this phone will dial, if Hotline is enabled
Phone Follows WAN	When enabled the phone will lose power any time the WAN is operation status of down. This will allow line monitoring equipment to detect loss of service.
Tx Path Gain (dB)	Transmit Gain of the upstream analog to digital path for phone to network.
Rx Path Gain (dB)	Receive Gain of the downstream analog to digital path for network to phone.
G.729A (ACELP)	The highest priority codec will be selected first if offered by the switch. If Do Not Use is selected. The G.729A (ACELP) codec will omit from the selection choice.
G.726 (ADPCM)	The highest priority codec will be selected first if offered by the switch. If Do Not Use is selected. The G.726 (ADPCM) codec will omit from the selection choice
G.711MuLaw (PCM)	The highest priority codec will be selected first if offered by the switch. If Do Not Use is selected. The G.711MuLaw (PCM) codec will omit from the selection choice
G.711ALaw (PCM)	The highest priority codec will be selected first if offered by the switch. If Do Not Use is selected. The G.711ALaw (PCM) codec will omit from the selection choice

VLAN

The VLAN page both creates and defines VLANs as well as assigns VLANs to available ports.

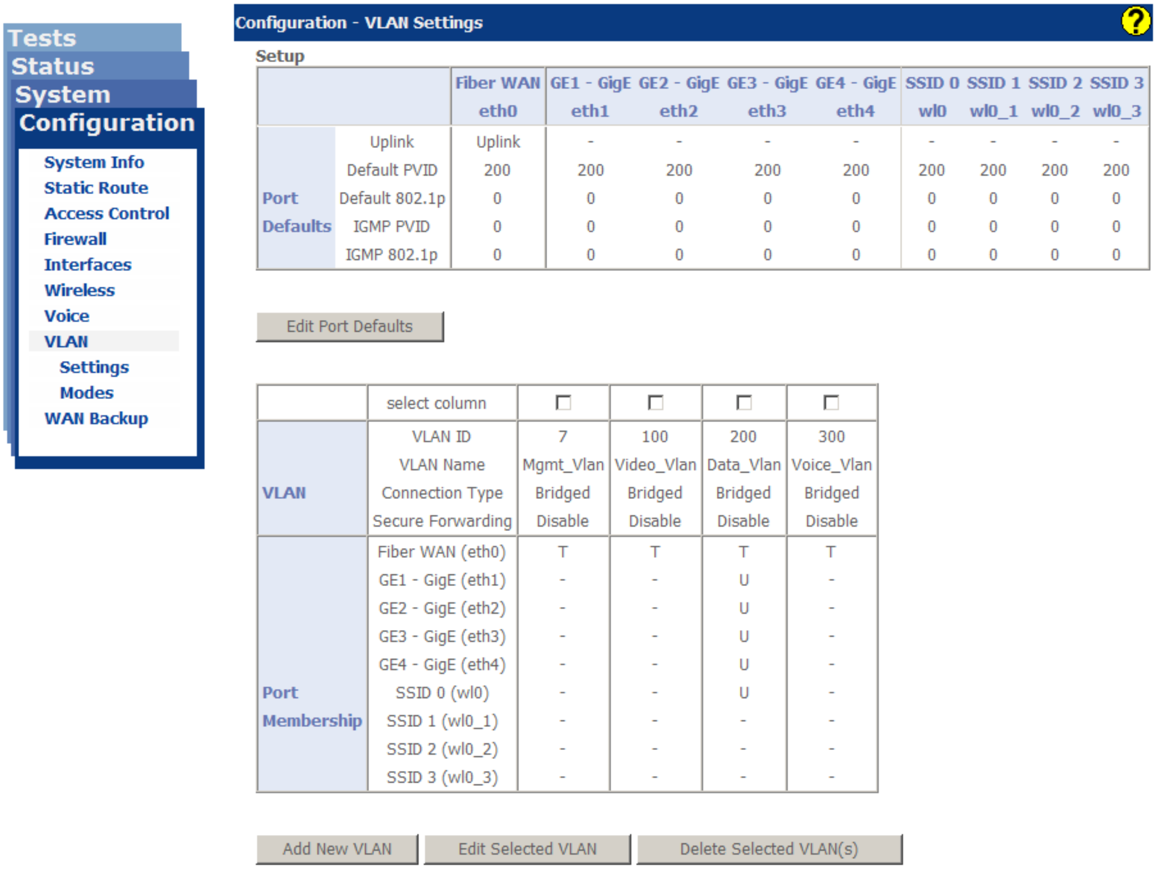
The VLAN screen has two tables — port defaults and VLANs and port membership.

For information about VLAN taggings, see *VLANS* on page 197.

Settings

The first table displays the configured **Port Defaults** including which interface has been configured to be the uplink, the default VLAN ID and 802.1p priority tag which will be applied to untagged traffic on ingress of each port, and the Port Filtering enable/disable per port.

Figure 108: Configuration | VLAN page



Configuration - VLAN Settings

Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSID 2 wl0_2	SSID 3 wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	Default PVID	200	200	200	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0	0

	select column	□	□	□	□
VLAN	VLAN ID	7	100	200	300
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	Connection Type	Bridged	Bridged	Bridged	Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-
	GE2 - GigE (eth2)	-	-	U	-
	GE3 - GigE (eth3)	-	-	U	-
	GE4 - GigE (eth4)	-	-	U	-
	SSID 0 (wl0)	-	-	U	-
	SSID 1 (wl0_1)	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-
	SSID 3 (wl0_3)	-	-	-	-

Table 51: Port Defaults

UI Label	Description
Port Type	Indicates which interface is accessing the global network (designated as Uplink).

Table 51: Port Defaults

UI Label	Description
Default PVID	The VLAN ID that will be inserted for any non tagged frames received on this interface. To remove tags in the upstream direction the port must be an untagged member of the same VLAN.
Default 802.1p	The default Quality of Service value for the PVID frames
IGMP PVID	The Vlan ID used in the VLAN tag that will be added to all non-tagged IGMP frames received on this interface.
IGMP 802.1.p	The default Class of Service value used in the VLAN tag that will be added to all non-tagged IGMP frames received on this interface.

The second table displays all configured VLANs in ascending order. For each VLAN, the configured Port Membership is displayed, along with configured VLAN Name, Connection Type, and Secure Forwarding Enable/Disable status.

Table 52: VLAN and Port Membership

UI Label	Description
VLAN ID	The VLAN ID for the column
VLAN Name	The VLAN Name as defined by the user for this VLAN ID
Connection Type	The type of VLAN the ONU was instructed to create during the add VLAN operation for this ID. This value CAN NOT be changed once created. The only option is to delete and recreate.
Secure Forwarding	Secure Forwarding causes all traffic to be forwarded to the uplink port. This prevents local port to port communication.
Port Membership	For each interface listed it indicates if this port is active for the configured VLAN

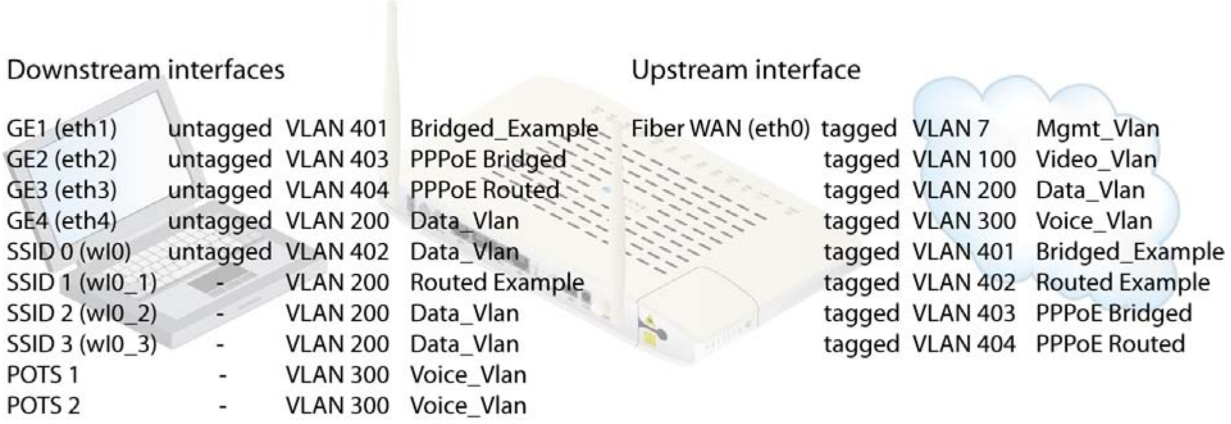
Edit Port Defaults

The **VLAN Settings | Edit Port Defaults** screen provides the means to define the VLAN ID and set 802.1p priorities for packets from each Ethernet port. This screen also sets which port is to be used as the WAN uplink.

The most common scenario is for a PC based subnet on a downstream port. The port receives the incoming untagged packet on the port and inserts the Port VLAN ID tag.

When the PVID is set to a specific VLAN it is to insert a VLAN tag for packets incoming on a downstream interface or directing (and stripping tags) to egress on a downstream interface. See *VLANS* on page 197 for more information and examples.

Figure 109: VLANs and interfaces used for examples



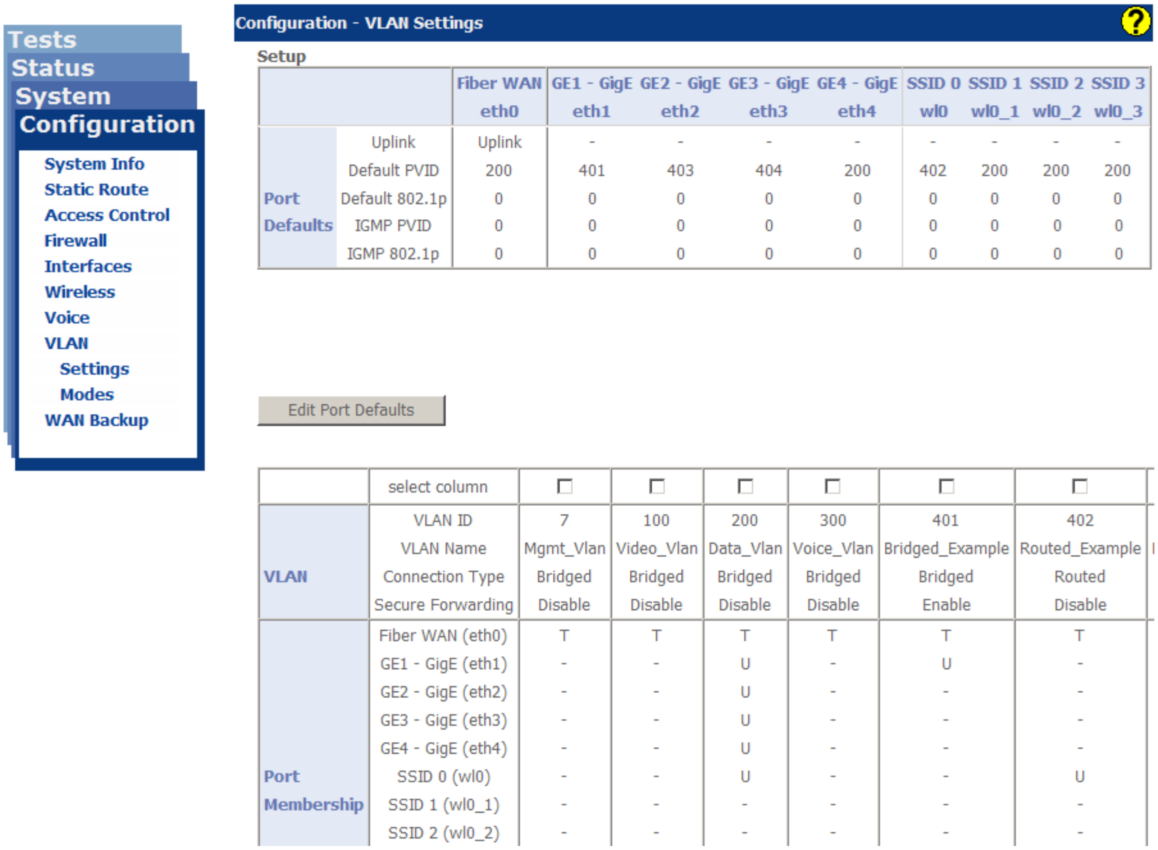
Downstream interfaces

GE1 (eth1)	untagged	VLAN 401	Bridged_Example
GE2 (eth2)	untagged	VLAN 403	PPPoE Bridged
GE3 (eth3)	untagged	VLAN 404	PPPoE Routed
GE4 (eth4)	untagged	VLAN 200	Data_Vlan
SSID 0 (wl0)	untagged	VLAN 402	Data_Vlan
SSID 1 (wl0_1)	-	VLAN 200	Routed Example
SSID 2 (wl0_2)	-	VLAN 200	Data_Vlan
SSID 3 (wl0_3)	-	VLAN 200	Data_Vlan
POTS 1	-	VLAN 300	Voice_Vlan
POTS 2	-	VLAN 300	Voice_Vlan

Upstream interface

Fiber WAN (eth0)	tagged	VLAN 7	Mgmt_Vlan
	tagged	VLAN 100	Video_Vlan
	tagged	VLAN 200	Data_Vlan
	tagged	VLAN 300	Voice_Vlan
	tagged	VLAN 401	Bridged_Example
	tagged	VLAN 402	Routed Example
	tagged	VLAN 403	PPPoE Bridged
	tagged	VLAN 404	PPPoE Routed

Figure 110: Example VLANs and interfaces



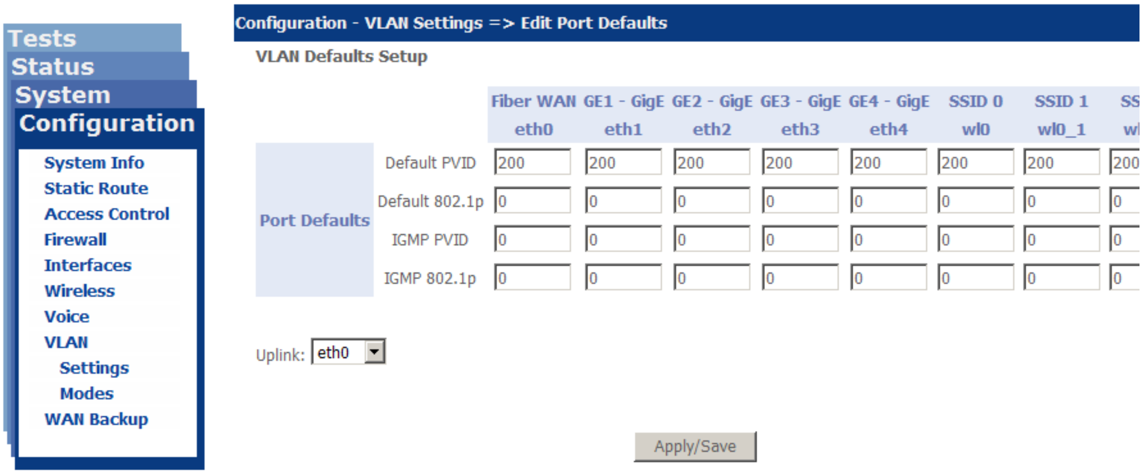
Configuration - VLAN Settings

Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSID 2 wl0_2	SSID 3 wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	Default PVID	200	401	403	404	200	402	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0	0

	select column	□	□	□	□	□	□
VLAN	VLAN ID	7	100	200	300	401	402
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan	Bridged_Example	Routed_Example
	Connection Type	Bridged	Bridged	Bridged	Bridged	Bridged	Routed
	Secure Forwarding	Disable	Disable	Disable	Disable	Enable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-	U	-
	GE2 - GigE (eth2)	-	-	U	-	-	-
	GE3 - GigE (eth3)	-	-	U	-	-	-
	GE4 - GigE (eth4)	-	-	U	-	-	-
	SSID 0 (wl0)	-	-	U	-	-	U
	SSID 1 (wl0_1)	-	-	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-	-	-

Figure 111: Setting port defaults



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SS w
Port Defaults	Default PVID	200	200	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

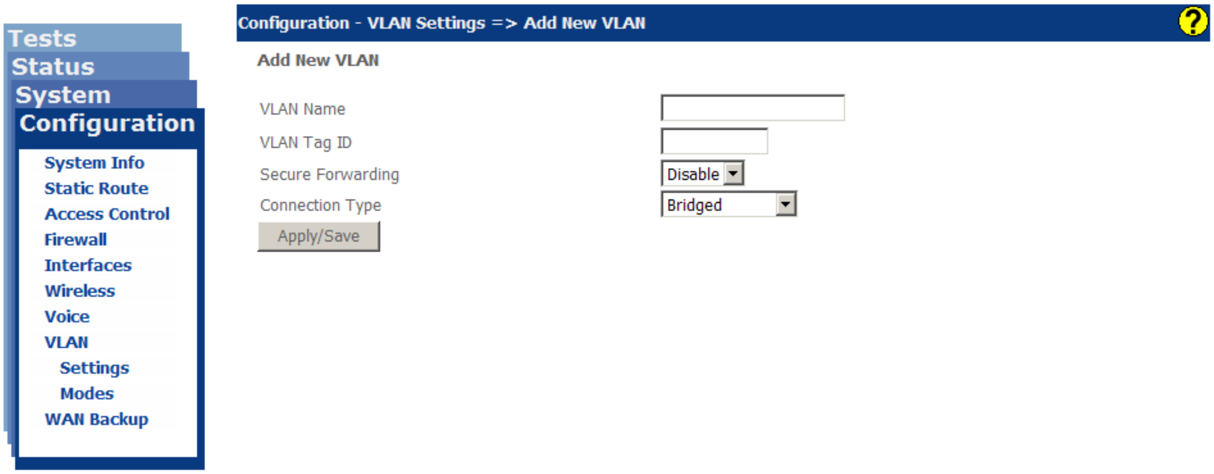
Table 53: Creating or editing port defaults

UI Label	Description
PVID	The VLAN ID that will be inserted for any non tagged frames received on this interface. ✓ **Note:** To strip the tag in the transmit (egress) direction, this port must be configured as an untagged member of the VLAN with a matching VLAN ID.
Default 802.1p	The default Quality of Service value for the PVID frames
IGMP PVID	The Vlan ID used in the VLAN tag that will be added to all non-tagged IGMP frames received on this interface.
IGMP 802.1.p	The default Class of Service value used in the VLAN tag that will be added to all non-tagged IGMP frames received on this interface.
Uplink	Selects which port is defined as an uplink for the zNID. Normally this would be eth0, the Fiber WAN port.

Add New VLAN

To add a new VLAN you define the name, the ID, whether secure forwarding is applied to the VLAN and whether the VLAN is bridged, routed, or for PPPoE.

Figure 112: Adding a new VLAN



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name

VLAN Tag ID

Secure Forwarding: Disable

Connection Type: Bridged

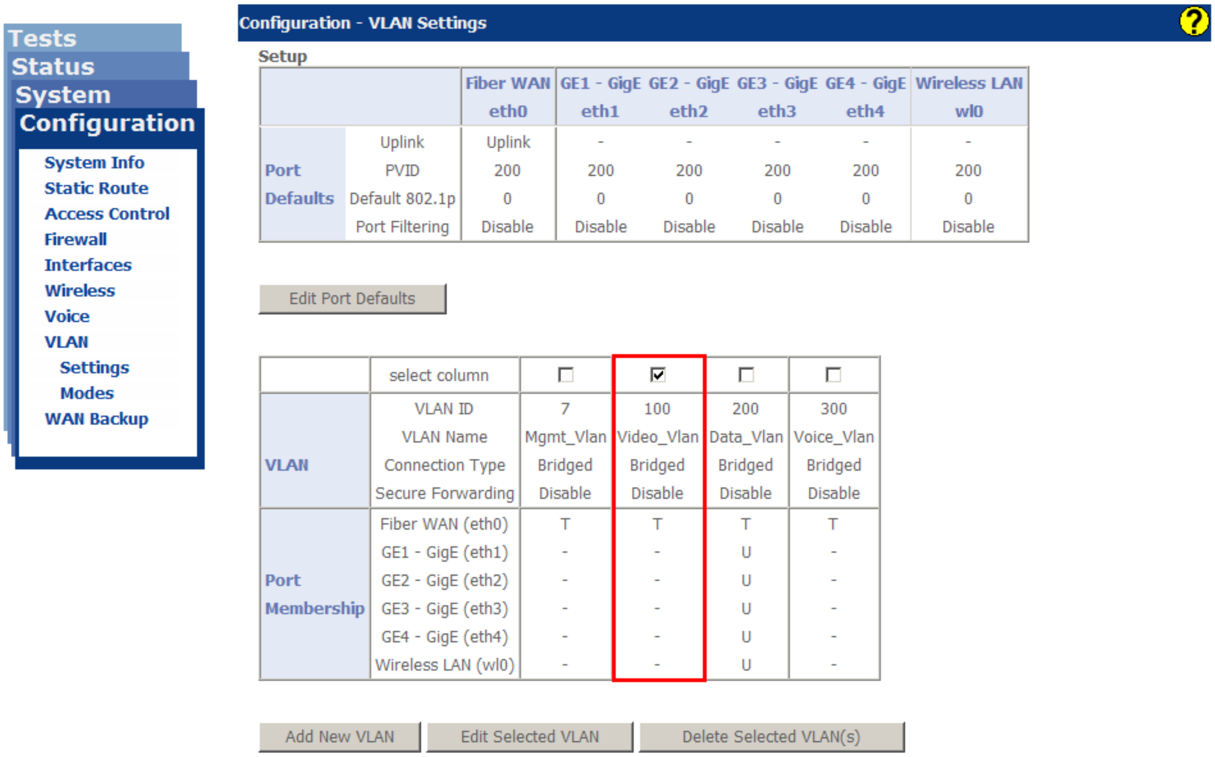
Table 54: Adding a VLAN

UI Label	Description
VLAN Name	A user defined name for this VLAN
VLAN ID	The VLAN ID
Secure Forwarding	Setting Secure Forwarding to Enabled will result in broadcast frames being discarded
Connection Type	The type of VLAN the ONU was instructed to create during the add VLAN operation for this ID. This value CAN NOT be changed once created. The only option is to delete and recreate. VLAN types: • Bridged (See *Bridged* on page 157) • Bridged via CPU or CPU-Bridged. (Bridging option for Dual Managed mode with VEIP, See *Bridged* on page 157) • Routed (See *Routed* on page 158) • Brouted (See *Brouted* on page 159) • PPPoE–Bridged (See *PPPoE Bridged or Routed* on page 160) • PPPoE–Routed (See *PPPoE Bridged or Routed* on page 160)

Edit Selected VLAN

Once a VLAN is created, you cannot change the name or VLAN ID, interface type and whether secure forwarding is applied to the VLAN. You can define port membership for an existing VLAN.

Figure 113: Selecting a VLAN for editing



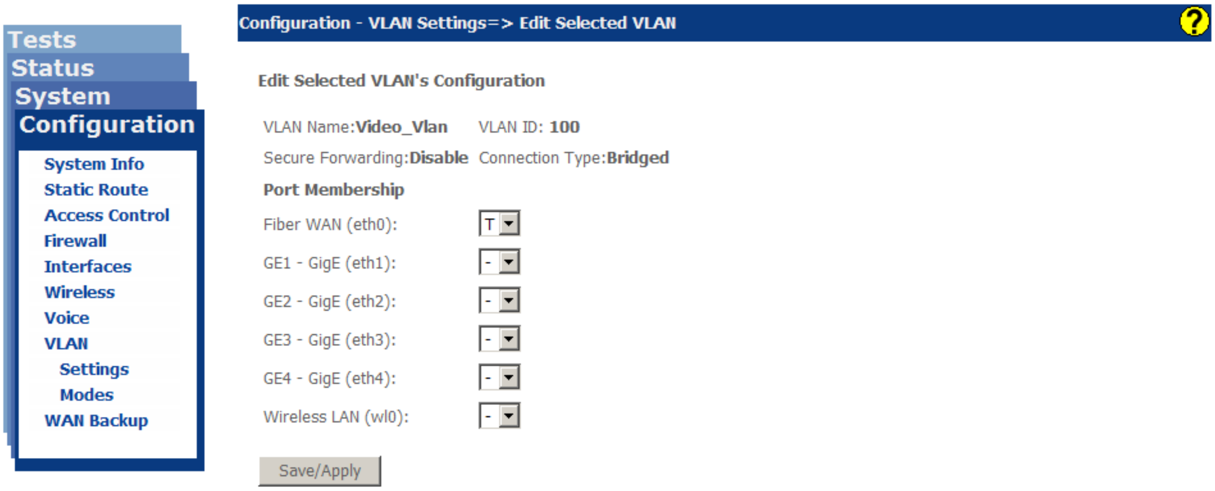
Configuration - VLAN Settings

Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	Wireless LAN wl0
Port Defaults	Uplink	Uplink	-	-	-	-	-
	PVID	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0
	Port Filtering	Disable	Disable	Disable	Disable	Disable	Disable

	select column	☐	☑	☐	☐
VLAN	VLAN ID	7	100	200	300
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	Connection Type	Bridged	Bridged	Bridged	Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-
	GE2 - GigE (eth2)	-	-	U	-
	GE3 - GigE (eth3)	-	-	U	-
	GE4 - GigE (eth4)	-	-	U	-
	Wireless LAN (wl0)	-	-	U	-

Figure 114: Editing port membership for an existing VLAN



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**Video_Vlan** VLAN ID: **100**

Secure Forwarding:**Disable** Connection Type:**Bridged**

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	-
GE3 - GigE (eth3):	-
GE4 - GigE (eth4):	-
Wireless LAN (wl0):	-

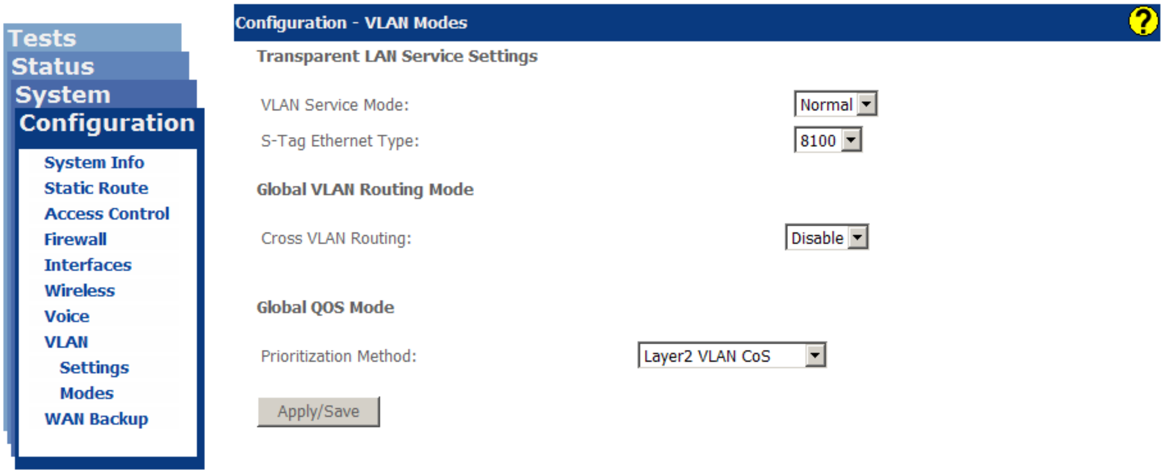
Table 55: In the VLAN editing screen, only the port membership for the VLAN may be defined

UI Label	Description
VLAN Name	The user defined name for this VLAN. **Once the VLAN is created this name cannot be changed. You must delete the VLAN and recreate it with a different name.**
VLAN ID	The VLAN ID. **Once the VLAN is created the VLAN ID cannot be changed. You must delete the VLAN and recreate it with a different VLAN ID.**
Secure Forwarding	Secure Forwarding set to Enabled results in broadcast frames being discarded. **Once the VLAN is created the VLAN ID cannot be changed. You must delete the VLAN and recreate it with a different VLAN ID.**
Connection Type	The type of VLAN the ONU was instructed to create during the add VLAN operation for this ID. This value CAN NOT be changed once created. The only option is to delete and recreate.
Port Membership	Assigns which ports will have the VLAN shown in VLAN ID.

Modes

The Transparent LAN Service Settings screen allows the TLS parameters to be set or modified.

Figure 115: Transparent LAN service settings



Configuration - VLAN Modes

Transparent LAN Service Settings

VLAN Service Mode: Normal

S-Tag Ethernet Type: 8100

Global VLAN Routing Mode

Cross VLAN Routing: Disable

Global QOS Mode

Prioritization Method: Layer2 VLAN CoS

Table 56: In the VLAN editing screen, only the port membership for the VLAN may be defined

UI Label	Description
VLAN Service Mode	• Normal All traffic must be encapsulated within a configured VLAN tag. Untagged traffic will be tagged upon LAN port ingress based on the configured Port Defaults. • S-Tag All traffic must be encapsulated within a configured S-Tag. Untagged or single-tagged traffic can be S-tagged upon LAN port ingress based on the configured Port Defaults.
S-Tag Ethernet Type	When S-Tag is selected, the S-Tag service type may be selected. The outer S-Tag is identified by a unique Tag Protocol Identifier (TPID). The IEEE standard value for the TPID is 88A8 (hex), however older product may use 8100, 9100, 9200, or 9300. The zNIDs provide support for interaction with these older devices. • 8100 • 88A8 • 9100 • 9200 • 9300

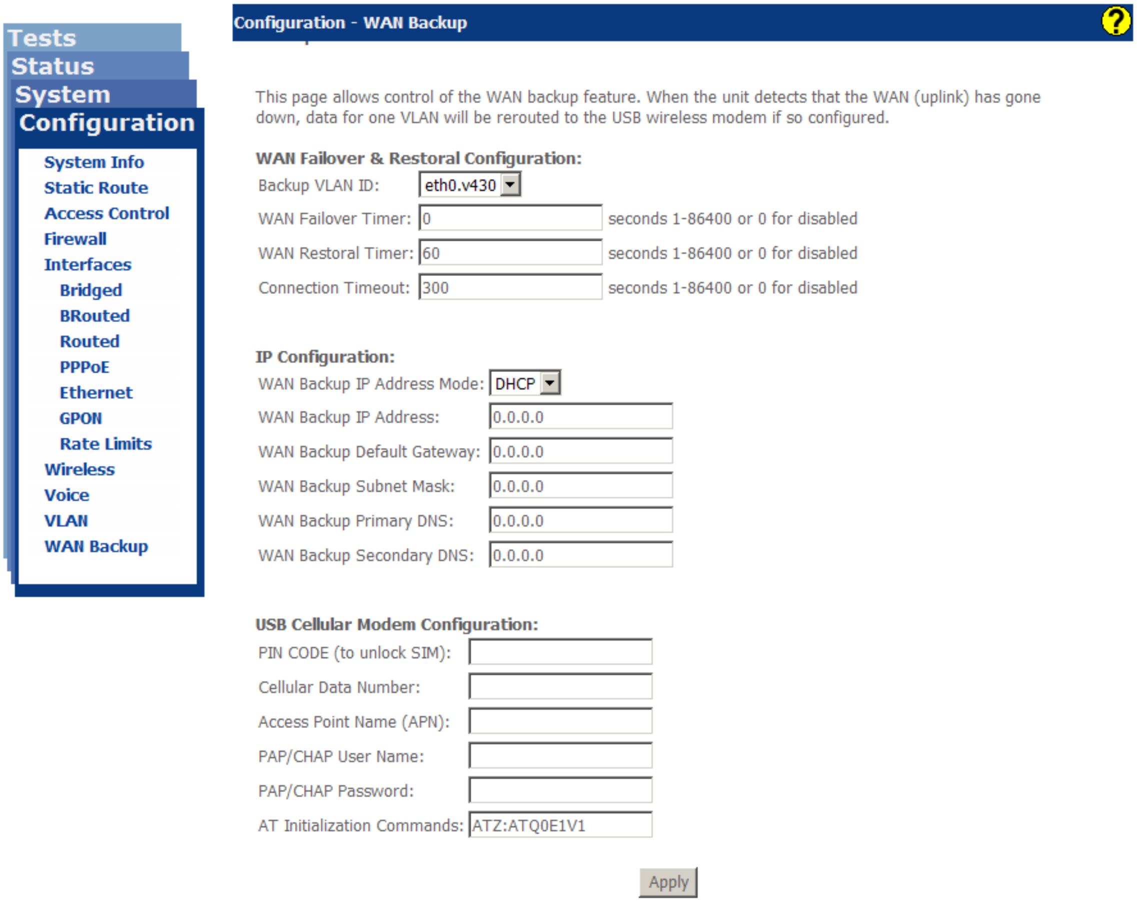
Table 56: In the VLAN editing screen, only the port membership for the VLAN may be defined

UI Label	Description
Cross VLAN Routing Mode	When **Enable** is selected routing between VLANs is allowed. • Enable Route table lookups ignore the VLAN ID of the ingress and egress ports. If there is a match, the packet is routed out the interface specified in the Route table, regardless of which VLAN it is a member of. (Cross VLAN Routing disabled is the default behavior.) • Disable Packets will be forwarded to the configured Default Route for the VLAN that they arrived on, unless there is a Route Table match within that same VLAN. Routing of packets across VLANs is prevented, providing traffic isolation.

WAN backup

With the WAN backup feature configured, if the WAN (uplink) has gone down, data for one VLAN can be rerouted to the USB wireless modem. WAN backup requires that at least one VLAN on the uplink has NAT enabled.

Figure 116: WAN backup configuration



This page allows control of the WAN backup feature. When the unit detects that the WAN (uplink) has gone down, data for one VLAN will be rerouted to the USB wireless modem if so configured.

WAN Failover & Restoral Configuration:

Backup VLAN ID:	eth0.v430	
WAN Failover Timer:	0	seconds 1-86400 or 0 for disabled
WAN Restoral Timer:	60	seconds 1-86400 or 0 for disabled
Connection Timeout:	300	seconds 1-86400 or 0 for disabled

IP Configuration:

WAN Backup IP Address Mode:	DHCP
WAN Backup IP Address:	0.0.0.0
WAN Backup Default Gateway:	0.0.0.0
WAN Backup Subnet Mask:	0.0.0.0
WAN Backup Primary DNS:	0.0.0.0
WAN Backup Secondary DNS:	0.0.0.0

USB Cellular Modem Configuration:

PIN CODE (to unlock SIM):	
Cellular Data Number:	
Access Point Name (APN):	
PAP/CHAP User Name:	
PAP/CHAP Password:	
AT Initialization Commands:	ATZ:ATQ0E1V1

Table 57: WAN backup configuration parameters

UI Label	Description
Backup VLAN ID	The USB Cellular modem sends/receives untagged packets, so they can be mapped into one and only one VLAN. This must be a Routed, Brouted, PPPoE-Bridged, or PPPoE-Routed VLAN with NAT Enabled. When the WAN uplink fails, traffic on this VLAN will be routed to/from the USB Cellular backup link.

Table 57: WAN backup configuration parameters

UI Label	Description
WAN Failover Timer	The WAN Failover timer is used to determine how long (in seconds) the Fiber uplink interface must be operationally DOWN before a USB Cellular WAN Backup connection will be initiated. The Default value is 0 seconds, which DISABLES this feature. Recommended value to enable this feature is 60 seconds.
WAN Restoral Timer	The WAN Restoral timer is used to determine how long (in seconds) the Fiber uplink interface must remain in an operational UP condition before the Cellular Backup connection will be terminated and the traffic that was being forwarded out the USB interface is forwarded to the 5xx GEM instead. The Default value is 60 seconds.
Connection Timeout	Specifies the duration of inactivity in seconds before the cellular data call will automatically terminate. A new call will be initiated automatically when a packet must be sent upstream on the designated VLAN if the WAN uplink is still Operationally DOWN. A value of 0 will DISABLE the Connection Timeout feature (Nailed Up mode). The default value is 360 seconds.
WAN Backup IP Address Mode	The WAN IP Address, Default Gateway IP, Subnet Mask, and DNS Server IP must all be defined for the USB Cellular Backup connection. When IP Address Mode is set to DHCP, a DHCP Request will be sent upstream after the Cellular Data Connection has been established to acquire this information dynamically. When the WAN Backup IP Address Mode is set to Static, this information must be statically configured.
WAN Backup Default Gateway	The IP Address to be used on the WAN uplink interface of a Cellular Backhaul connection. Acquired dynamically in DHCP mode.
WAN Backup Subnet Mask	The Subnet Mask to used on the WAN uplink interface of a Cellular Backhaul connection. Acquired dynamically in DHCP mode.
WAN Backup Primary DNS	The Subnet Mask to used on the WAN uplink interface of a Cellular Backhaul connection. Acquired dynamically in DHCP mode.

Table 57: WAN backup configuration parameters

UI Label	Description
WAN Backup Secondary DNS	The IP Address of the Secondary DNS Server to be used on the WAN uplink interface of a Cellular Backhaul connection. Acquired dynamically in DHCP mode.
PIN	Four digit Personal Identification Number (PIN) code used to unlock the SIM card. For GPRS/UMTS networks, *99# is typically used. For CDMA/EVDO networks. #777 is typically used.
Access Point Name (APN)	Text string up to 31 characters in length defining the Access Point Name for connections to the GPRS/ UMTS network. Provided by the ISP. For example: epc.tmobile.com
PAP/CHAP User Name	Required for CHAP or PAP authentication. Leave blank if CHAP or PAP is not used.
PAP/CHAP Password	Required for CHAP or PAP authentication. Leave blank if CHAP or PAP is not used.
AT Initialization Commands	Any additional AT commands that must be sent to the USB Cellular Modem prior to initiating the call may be entered here. For example: ATZ:ATQ0E1V1.

Deployment scenarios

The connection type for each VLAN can be configured for Bridged, Routed, Brouted, PPPoE Bridged, or PPPoE Routed.

For a discussion of the differences among the connection types please see IP configuration options, page 157.

Creating data connections follows a different procedure than voice connections.

- *Creating data connections* on page 162
- *Creating bridge connections* on page 163
- *Creating routed connections* on page 166
- *Creating brouted connections* on page 172
- *Creating PPPoE tunnels* on page 179
  - *PPPoE Bridged* on page 179
  - *PPPoE Routed* on page 184
- *Creating wireless connections* on page 188
- *Creating voice connections* on page 191
  - *SIP* on page 191
  - *SIP-PLAR* on page 192
  - *MGCP* on page 193
- *Creating Dual Managed connections* on page 194

Other features: more information and additions

- *VLANS* on page 197
- *NAT and DHCP* on page 205
- *DHCP server* on page 209
- *Data services* on page 210
  - *Rate limiting* on page 210
  - *Priority* on page 211
  - *CoS* on page 211

IP configuration options

The different bridge types which the zNID 24xx supports provides present different options for assigning IP addresses.

- Bridged

  For bridged VLANs, an IP Address can be assigned if the zNID will be a host in a particular IP subnet.

  – IP addresses for LAN-side client devices can be statically assigned or assigned by an upstream DHCP server.

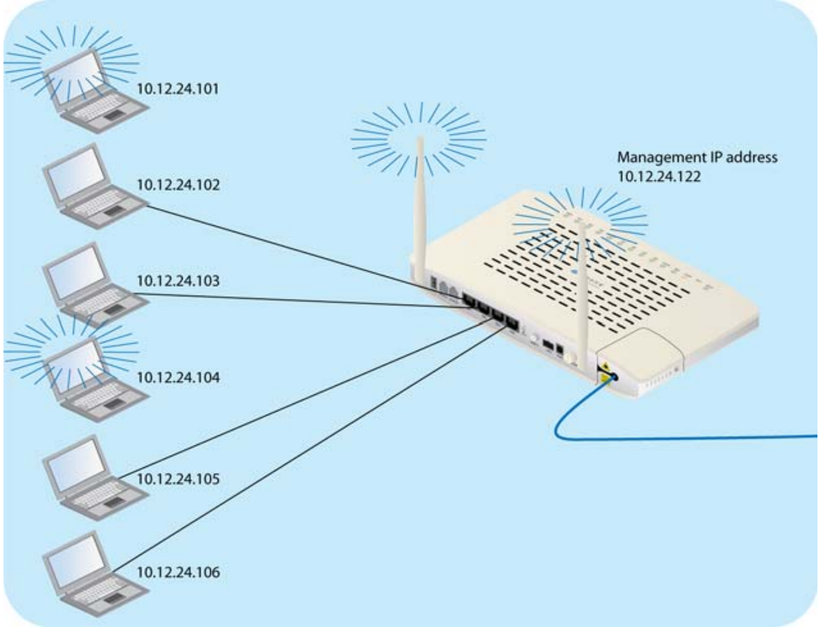
  – Any number of Ethernet ports or WiFi SSIDs can be members of the Bridged VLAN

  – All clients in a bridged VLAN will be in the same IP subnet, and the zNID 24xx will enable direct local peer-to-peer communications between all clients unless the Secure Forwarding option has been enabled.

    If Secure Forwarding is enabled, all broadcast traffic is forwarded upstream and not flooded out the other local ports in the VLAN. This prevents local peer-to-peer communications, and is equivalent to the ONU operating mode

  – Bridged with CPU or CPU-Bridged must be selected for using bridged VLANs in Dual Managed mode with VEIP

Figure 117: For bridged connections all the interfaces are in the same subnet



See Creating bridge connections, page 163 for the procedures for creating bridged connections.

- Routed

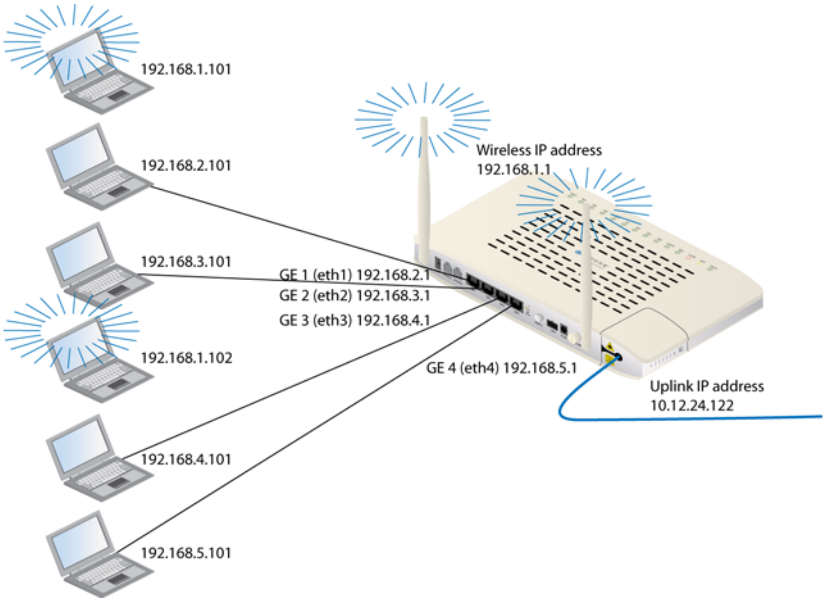
  For Routed VLANs, an IP Address will be assigned per physical port that is assigned to the VLAN. The minimum configuration will have the uplink interface and at least one LAN-side interface. When there are multiple LAN ports in the same Routed VLAN, each one must be assigned its own IP subnet.

  – In the illustration below, a NAT Routed VLAN has been configured that contains three LAN ports and one SSID. A total of six IP addresses are assigned to the 2426 for this configuration. A WAN IP address is assigned to the uplink, and four LAN-side IP addresses must be assigned, each in a separate subnet, plus an IP subnet for the WiFi interface.

  – All Wi-Fi connected client devices will be in the same subnet. An RG configuration item called “Isolate Clients” in the Wireless / Basic menu determines if these devices will be able to communicate locally with each other, or if all traffic will be forwarded upstream. When Isolate Clients is enabled, all traffic is forwarded upstream, blocking local peer-to-peer communications.

  – The example below shows a Routed VLAN with NAT. When NAT is enabled, the Router performs Network Address Translation, mapping each LAN side IP address and source port to a unique protocol port used with the WAN IP Address for communications across the network.

Figure 118: For routed connections each interface is in its own subnet



See Creating routed connections, page 166 for the procedures for creating routed connections.

- Brouted

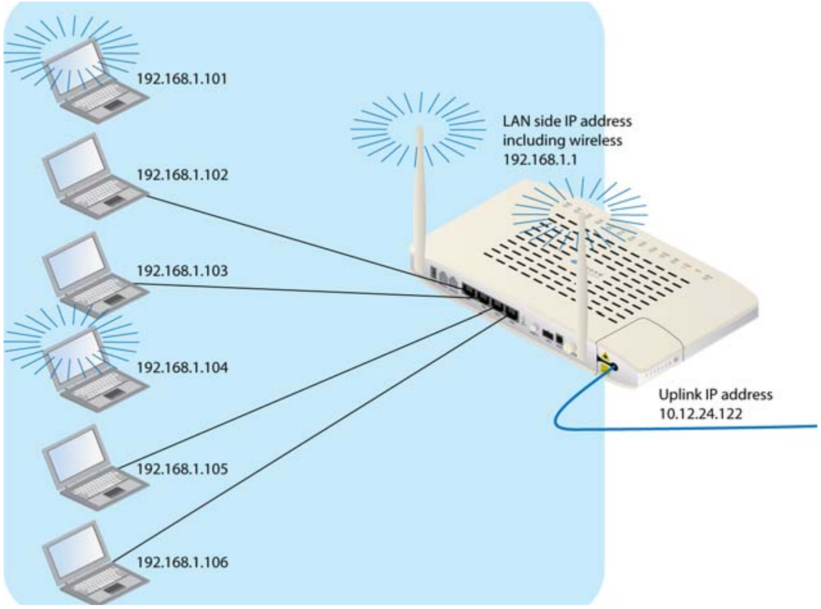
  For Brouted VLANs, there are only two IP interfaces - one for the Routed uplink interface and a second for the Bridged LAN-side interface. A Brouted VLAN may have multiple LAN ports as members, and all ports will use the same IP subnet. So Brouted means that the LAN side is like a bridge, but has a routed interface for the WAN side.

  – Brouted VLANs enable local peer-to-peer communications between all client devices, just like Bridged VLANs do. All clients will have IP Addresses in the same subnet.

  – A DHCP Server may be configured in the zNID 24xx to automatically assign local IP addresses in the assigned subnet.

  – NAT is typically enabled on a Brouted VLAN, using private IP Addresses locally and a single public IP address on the uplink interface

Figure 119: For brouted all LAN side interfaces are in one subnet. The uplink is in another subnet


192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.106
LAN side IP address including wireless 192.168.1.1
Uplink IP address 10.12.24.122

See Creating brouted connections, page 172 for the procedures for creating brouted connections.

- PPPoE Bridged or Routed

  PPPoE bridged or routed connections are very similar to bridged or routed connections, only that the uplink interface is a PPPoE client that establishes a PPPoE tunnel to an upstream BRAS

  – PPPoE/Bridged VLANs are similar to Brouted VLANs, but the uplink interface is a PPPoE client that establishes a PPPoE tunnel to an upstream BRAS. On the LAN side of a PPPoE/Bridged VLAN, all ports will be members of the same IP Subnet.

  – PPPoE/Routed VLANs are similar to Routed VLANs, but the uplink interface is a PPPoE client that establishes a PPPoE tunnel to an upstream BRAS. On the LAN side of a PPPoE/Routed VLAN, each LAN port will require its own IP subnet.

Figure 120: For PPPoE bridged the LAN side interfaces are all in the same subnet. The WAN side is in its own subnet and a PPPoE tunnel is created to an upstream BRAS

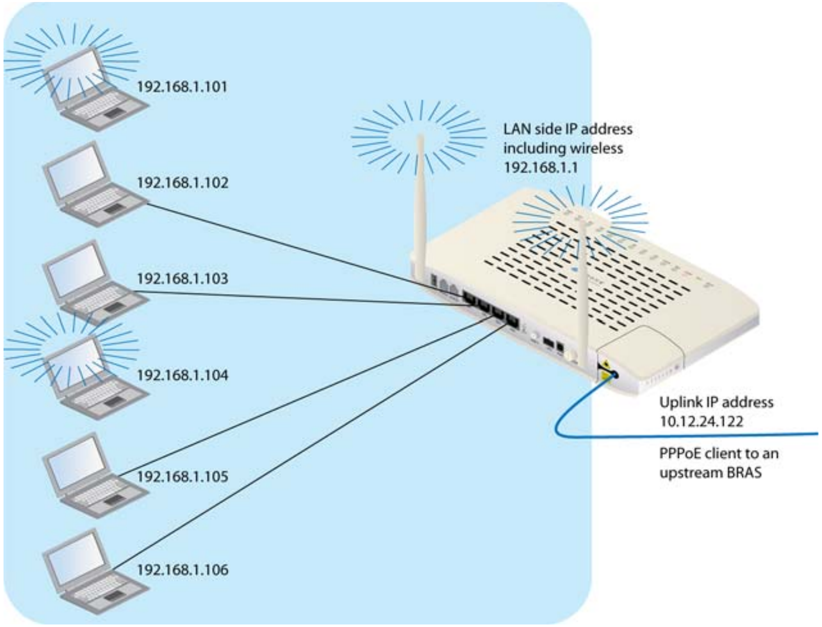
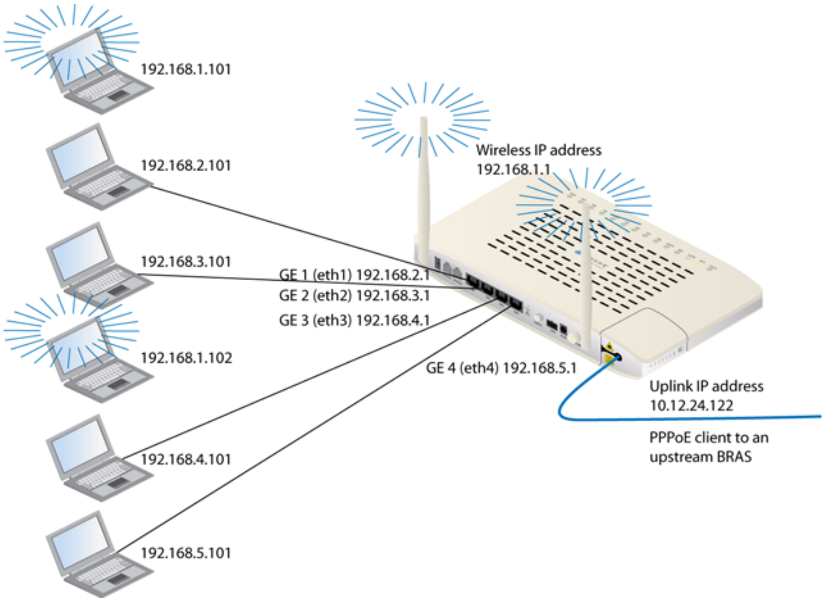


Figure 121: For PPPoE routed the LAN side interfaces are all their own subnets. The WAN side is in its own subnet and a PPPoE tunnel is created to an upstream BRAS



See Creating PPPoE tunnels, page 179 for the procedures for creating PPPoE tunnels.

Creating data connections

All connections, including voice and video, are based on the VLAN and all follow a general procedure:

1 Create VLAN

This first step is the same for all data connections, except for choosing which connection type. You name the connection and give it a VLAN ID as well as defining the connection type.

For voice configurations you select Bridged as the connection type and bind the POTS interface to the VLAN later in the process.

2 Select ports and set port defaults

This step is also the same for all connection types.

For wireless you would select the wireless interface as one of the ports, then later configure the wireless.

For OMCI & RG combined VEIP connections select “O” for the uplink port member.

3 Adjust WAN settings (Routed, Brouted and PPPoE connections)

This step configures the upstream interface.

For routed connections it defines the zNID device’s addressing and whether NAT (Network Address Translation) or DHCP Relay is used for the client devices on the LAN side.

For video connections you would enable IGMP snooping in this step.

For PPPoE connections this step has a PPPoE address mode used for defining the IP address for the zNID side of the PPPoE tunnel.

4 Adjust LAN settings (Routed, Brouted and PPPoE connections)

This step configure the downstream interface

For routed connections it defines whether the zNID is acting as a DHCP server for the client devices and creating a subnet.

For PPPoE connections Network Address Translation is required.

5 Configure wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options.

6 Select voice connection (Voice connections only)

For voice connections you select which of the configured VLANs to which to bind the POTS interface.

Creating bridge connections

In Bridged mode, the zNID 24xx operates as a standard learning bridge. The source addresses in received packet headers are examined to locate unknown devices. Until the location of the destination is known, the packets are flooded to all ports that are members of the VLAN. Once a device has been located, its location is recorded in a table where the MAC address is stored so as to preclude the need for further flooding.

In addition, there is a "secure forwarding" mode. When this mode is enabled, packets are not flooded to all ports. Instead, all packets are forwarded to the port that is designated as the uplink port. In this mode, users are prevented from directly communicating with each other.

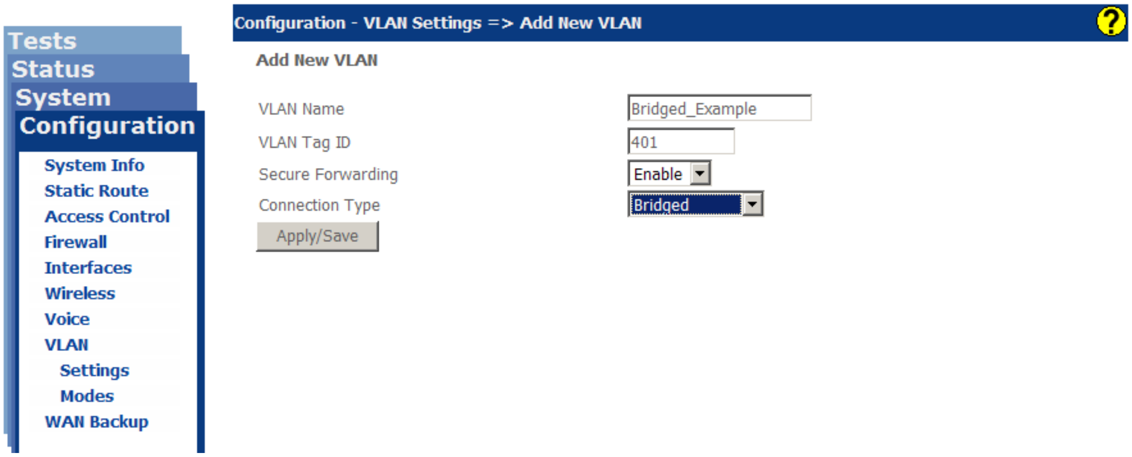
Note: Bridged connections for use with VEIP must use the CPU-Bridged type. See *Creating Dual Managed connections* on page 194 for an example creating

a CPU-Bridged type for VEIP.

To create a bridged connection

1 Create VLAN

Figure 122: Creating a bridged VLAN



Add New VLAN

VLAN Name	Bridged_Example
VLAN Tag ID	401
Secure Forwarding	Enable
Connection Type	Bridged

Apply/Save

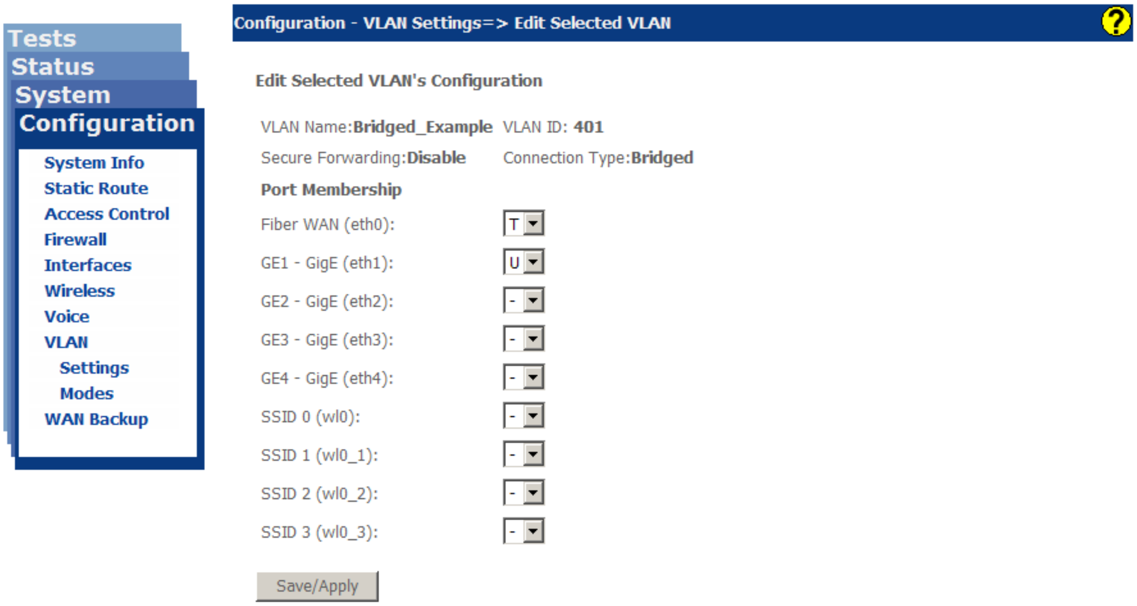
- **a** On the **Configuration|VLAN Settings** page, click **Add New VLAN**
- **b** In the **VLAN Name** text box enter a name for the VLAN
- **c** In the **VLAN Tag ID** text box enter a VLAN ID
- **d** <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

  See *Add New VLAN* on page 148 for more information
- **e** From the **Connection Type** dropdown select **Bridged**
- **f** Click **Apply/Save**

2 Select ports and set port defaults

a From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 123: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**Bridged_Example** VLAN ID: **401**

Secure Forwarding:**Disable** Connection Type:**Bridged**

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	U
GE2 - GigE (eth2):	-
GE3 - GigE (eth3):	-
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown

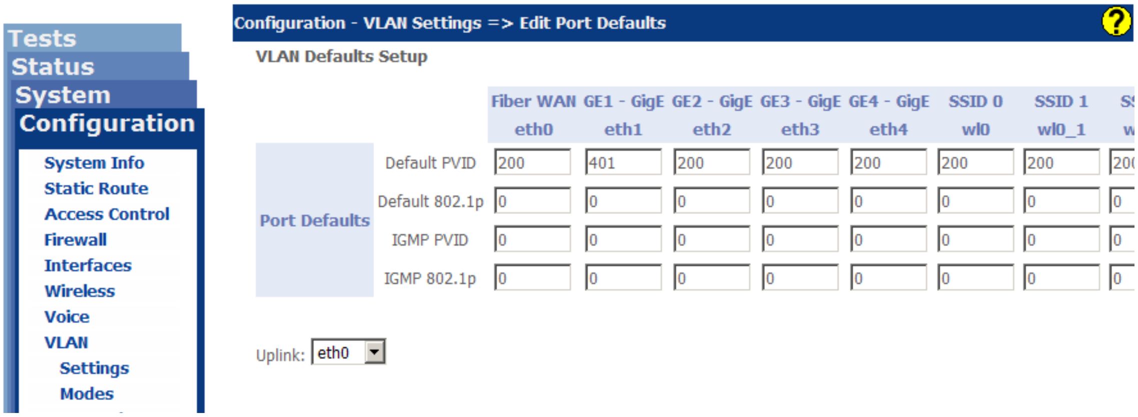
In this example we are only selected one untagged downstream interface. Select **U** from the **GE1 - GigE (eth1)** dropdown

b Click **Save/Apply**

c From the **VLAN | Settings** page click **Edit Port Defaults**

d In the **PVID** text box for **GE1 - GigE eth1**, enter 401 (the same as the ID for the VLAN)

Figure 124: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SS w
Port Defaults	Default PVID	200	401	200	200	200	200	200	20(
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

f Click **Save/Apply**

3 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

Creating routed connections

VLANs can be configured as Routed. With this connection type, packets are forwarded based on the destination IP address. Explicit routes can be configured or the system can use the default route, which is the next hop gateway for the VLAN. A total of 32 routes can be defined.

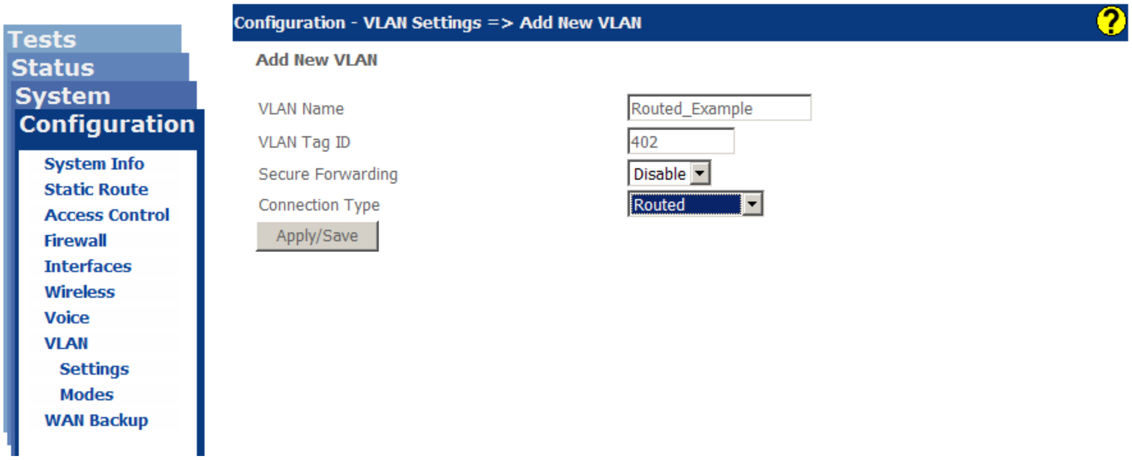
When in the Routed mode, additional features are enabled such as filtering (See *MAC filter* on page 126), and the DHCP server function (See *DHCP server* on page 209).

To create a routed connection

1 Create VLAN

This first step is the same for all data connections, except for choosing which connection type. You name the connection and give it a VLAN ID as well as defining the connection type.

Figure 125: Creating a routed VLAN



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name: Routed_Example
VLAN Tag ID: 402
Secure Forwarding: Disable
Connection Type: Routed

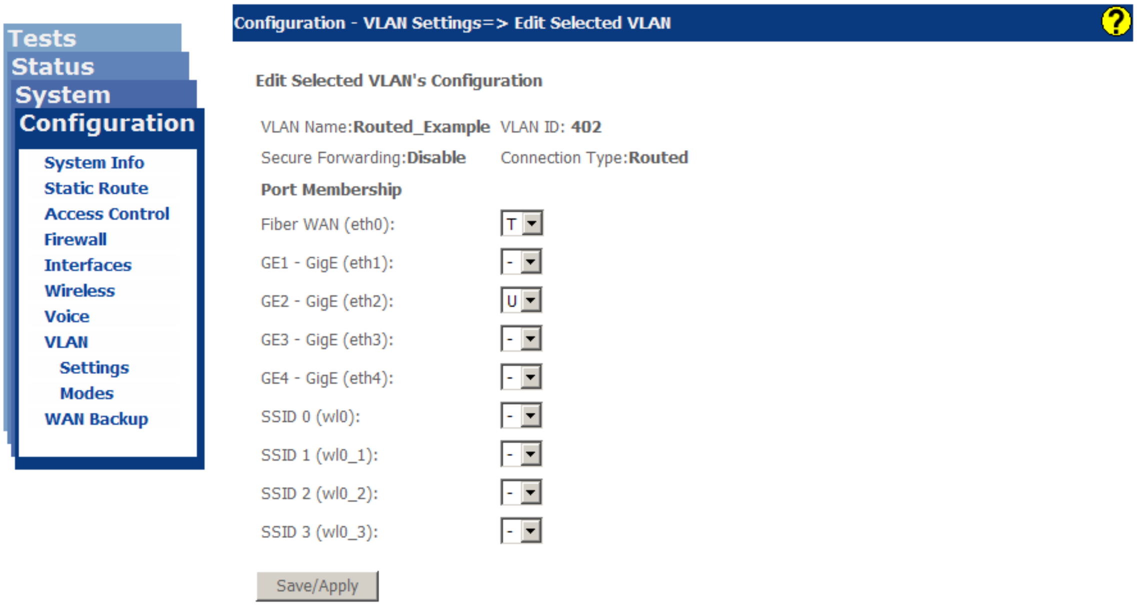
- **a** On the **Configuration|VLAN Settings** page, click **Add New VLAN**
- **b** In the **VLAN Name** text box enter a name for the VLAN
- **c** In the **VLAN Tag ID** text box enter a VLAN ID
- **d** <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

  See *Add New VLAN* on page 148 for more information
- **e** From the **Connection Type** dropdown select **Routed**
- **f** Click **Apply/Save**

2 Select ports and set port defaults

- **a** From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 126: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**Routed_Example** VLAN ID: **402**

Secure Forwarding:**Disable** Connection Type:**Routed**

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	U
GE3 - GigE (eth3):	-
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Save/Apply

Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown.

In this example we are only selected one untagged downstream interface. Select **U** from the **GE2 - GigE (eth2)** dropdown.

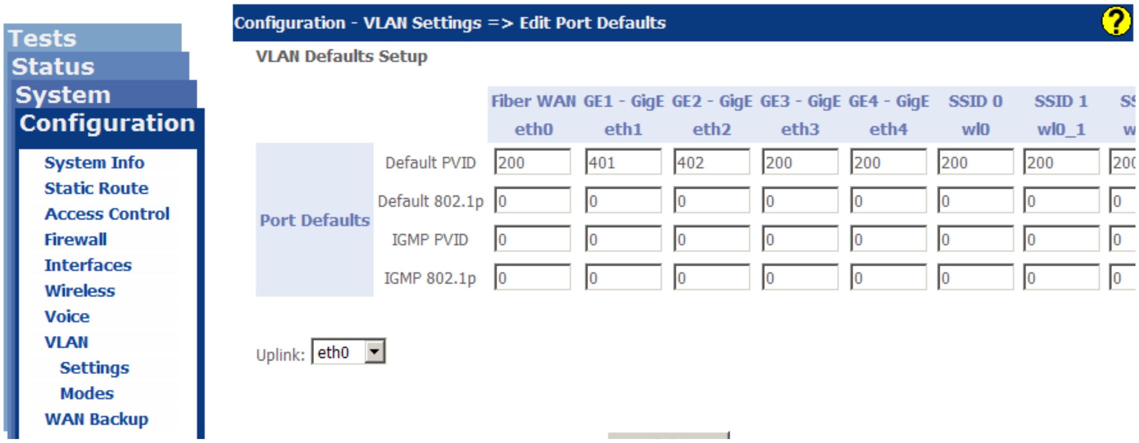
For Dual Managed connections that map to the VEIP select “O” for the uplink port member.

b Click **Save/Apply**

c From the **VLAN | Settings** page click **Edit Port Defaults**

d In the **PVID** text box for **GE2 - GigE eth2**, enter 402 (the same as the ID for the VLAN)

Figure 127: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SS w
Port Defaults	Default PVID	200	401	402	200	200	200	200	20
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

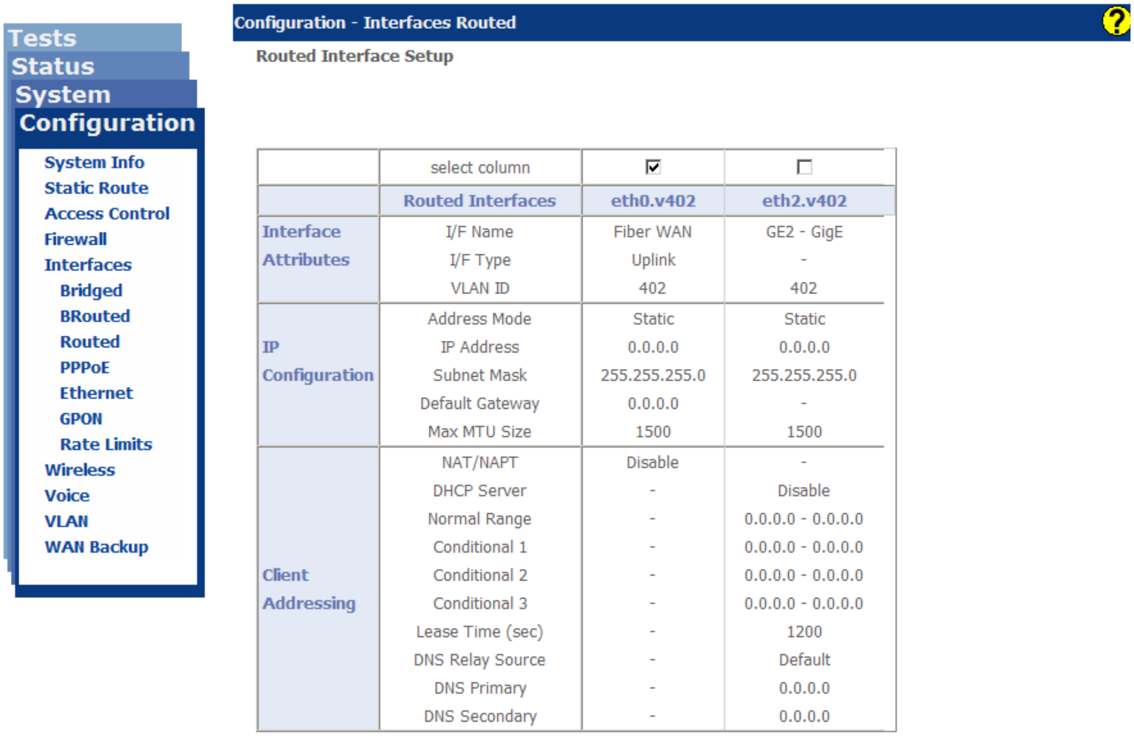
f Click **Save/Apply**

3 Adjust WAN settings

First we will set the addressing for the zNID on the upstream interface. Then we will set the NAT and DNS relay options for downstream devices.

a From the **Interfaces | Routed** page enter a check in the select column for eth0.v402, then click **Edit Selected Interface**

Figure 128: Selecting the fiber WAN interface for the VLAN



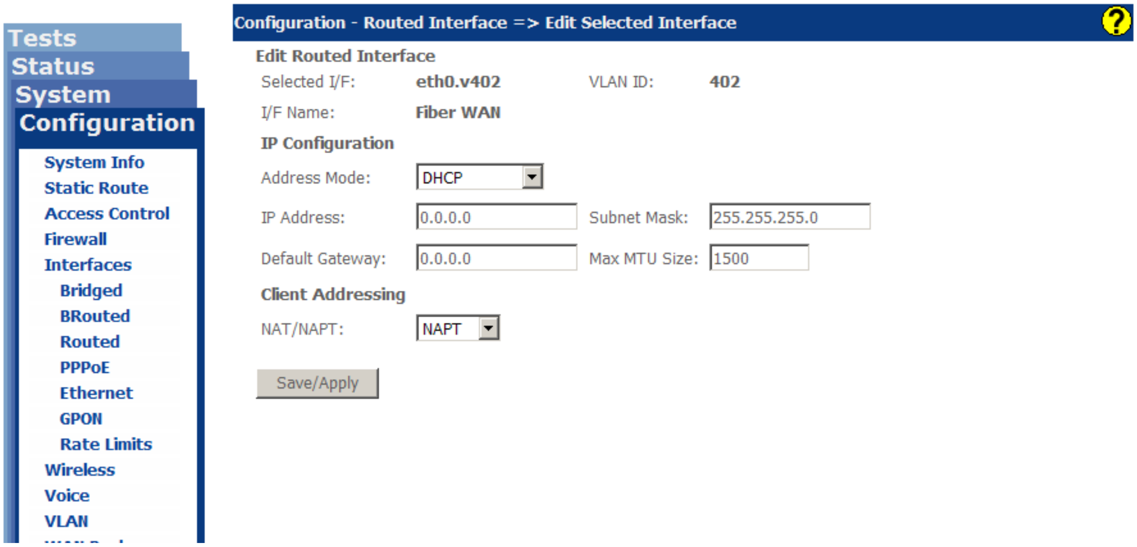
Configuration - Interfaces Routed

Routed Interface Setup

	select column	☑	□
	Routed Interfaces	eth0.v402	eth2.v402
Interface Attributes	I/F Name	Fiber WAN	GE2 - GigE
	I/F Type	Uplink	-
	VLAN ID	402	402
IP Configuration	Address Mode	Static	Static
	IP Address	0.0.0.0	0.0.0.0
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	Disable	-
	DHCP Server	-	Disable
	Normal Range	-	0.0.0.0 - 0.0.0.0
	Conditional 1	-	0.0.0.0 - 0.0.0.0
	Conditional 2	-	0.0.0.0 - 0.0.0.0
	Conditional 3	-	0.0.0.0 - 0.0.0.0
	Lease Time (sec)	-	1200
	DNS Relay Source	-	Default
	DNS Primary	-	0.0.0.0
	DNS Secondary	-	0.0.0.0

b In the **Configuration - Routed Interface --> Edit Selected Interface** page from the IP Configuration section **Address Mode** dropdown select **DHCP**.

Figure 129: Adjusting WAN settings: device addressing and NAT and DNS relay for clients



Configuration - Routed Interface => Edit Selected Interface

Edit Routed Interface

Selected I/F: eth0.v402 VLAN ID: 402

I/F Name: Fiber WAN

IP Configuration

Address Mode: DHCP

IP Address: 0.0.0.0 Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0 Max MTU Size: 1500

Client Addressing

NAT/NAPT: NAPT

For this example the ZNID will be getting its address from an upstream DHCP server.

Other options for device addressing:

- To assign a permanent IP to the zNID, select **Static** from the **Address Mode** dropdown

  You will need to get the **IP Address** from your ISP as well as the **Subnet Mask**, **Default Gateway** address and **DNS**.

- **Unconfigured**

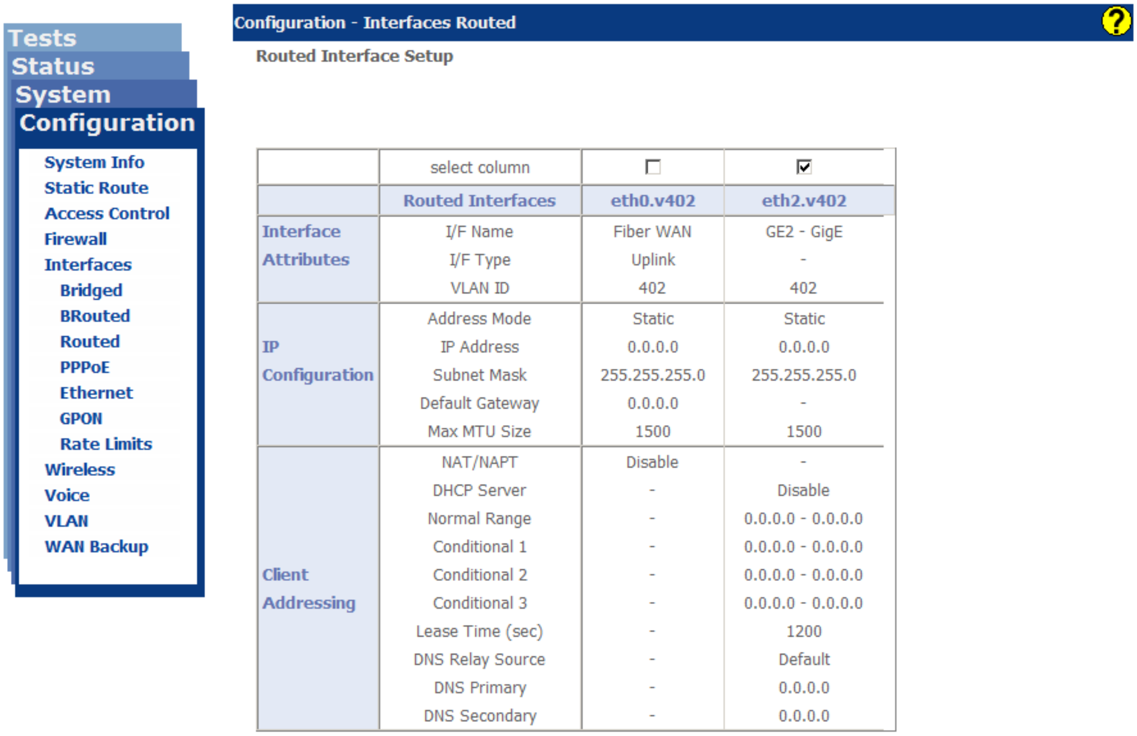
c From the **NAT/NAPT** dropdown select **NAPT**

For this example we are going to have private addresses for the downstream devices using Network Address Translation/ Network Address and Port Translation.

4 Adjust LAN settings

a From the **Interfaces | Routed** page enter a check in the select column for eth2.v402, then click **Edit Selected Interface**

Figure 130: Selecting the LAN interface for the VLAN



Configuration - Interfaces Routed

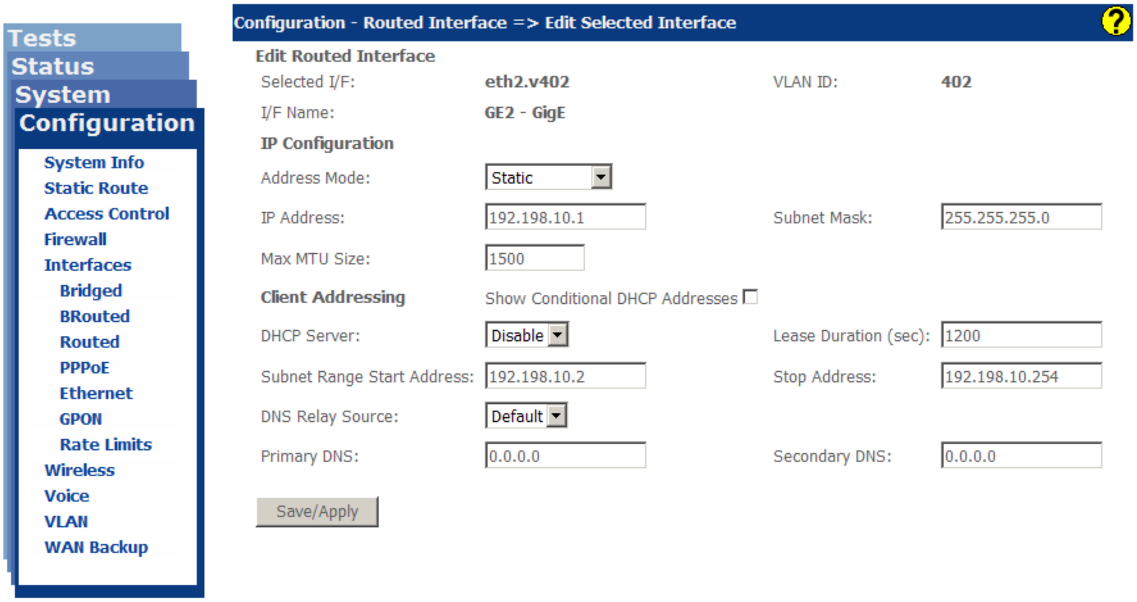
Routed Interface Setup

	select column	☐	☑
	Routed Interfaces	eth0.v402	eth2.v402
Interface Attributes	I/F Name	Fiber WAN	GE2 - GigE
	I/F Type	Uplink	-
	VLAN ID	402	402
IP Configuration	Address Mode	Static	Static
	IP Address	0.0.0.0	0.0.0.0
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	Disable	-
	DHCP Server	-	Disable
	Normal Range	-	0.0.0.0 - 0.0.0.0
	Conditional 1	-	0.0.0.0 - 0.0.0.0
	Conditional 2	-	0.0.0.0 - 0.0.0.0
	Conditional 3	-	0.0.0.0 - 0.0.0.0
	Lease Time (sec)	-	1200
	DNS Relay Source	-	Default
	DNS Primary	-	0.0.0.0
	DNS Secondary	-	0.0.0.0

b From the **Configuration - Routed Interface => Edit Selected Interface** page, select **Static** from the Address Mode dropdown below **IP Configuration**

For this example we are defining the IP address for the downstream interface, by selecting **Static**.

Figure 131: Selecting the fiber WAN interface for the VLAN



Configuration - Routed Interface => Edit Selected Interface

Edit Routed Interface

Selected I/F:	eth2.v402	VLAN ID:	402
I/F Name:	GE2 - GigE		

IP Configuration

Address Mode:	Static		
IP Address:	192.198.10.1	Subnet Mask:	255.255.255.0
Max MTU Size:	1500		

Client Addressing — Show Conditional DHCP Addresses □

DHCP Server:	Disable	Lease Duration (sec):	1200
Subnet Range Start Address:	192.198.10.2	Stop Address:	192.198.10.254
DNS Relay Source:	Default		
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0

The other options are

- DHCP
- Unconfigured

5 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

Creating brouted connections

Brouted VLANs enable local peer-to-peer communications between client devices, like bridged VLANs, but has a routed VLAN for the uplink interface.

Network Address Translation is typically enabled for Brouted VLANs using private IP addresses locally and a single IP address on the uplink interface.

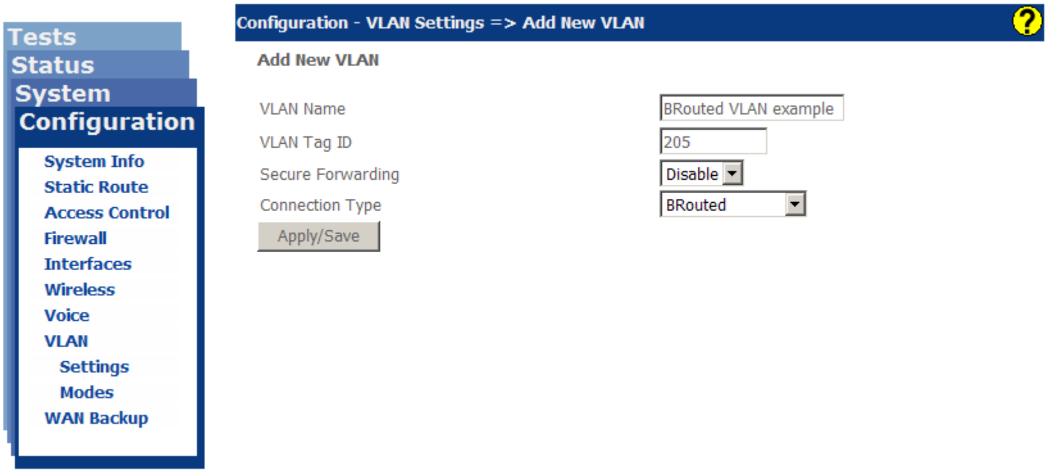
When in the Brouted mode, a DHCP server may be configured to automatically assign local IP addresses (See *DHCP server* on page 209).

To create a brouted connection

1 Create VLAN

This first step is the same for all data connections, except for choosing which connection type. You name the connection and give it a VLAN ID as well as defining the connection type.

Figure 132: Creating a routed VLAN



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name	BRouted VLAN example
VLAN Tag ID	205
Secure Forwarding	Disable
Connection Type	BRouted

a On the **Configuration|VLAN Settings** page, click **Add New VLAN**

b In the **VLAN Name** text box enter a name for the VLAN

c In the **VLAN Tag ID** text box enter a VLAN ID

d <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

See *Add New VLAN* on page 148 for more information

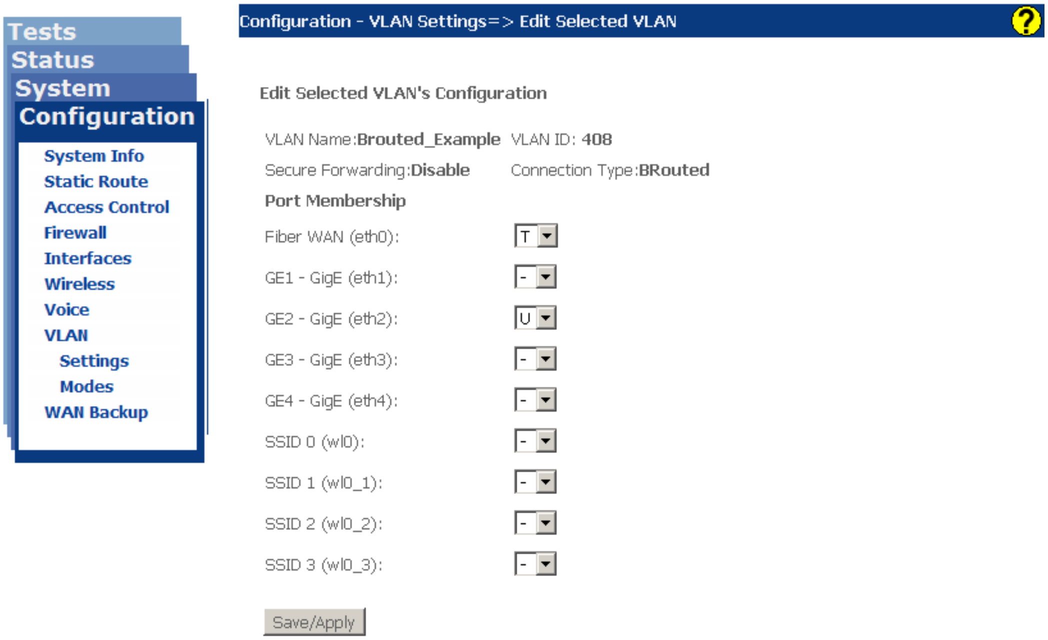
e From the **Connection Type** dropdown select **BRouted**

f Click **Apply/Save**

2 Select ports and set port defaults

a From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 133: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:Brouted_Example VLAN ID: 408

Secure Forwarding:Disable Connection Type:BRouted

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	U
GE3 - GigE (eth3):	-
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown.

In this example we are only selected one untagged downstream interface. Select **U** from the **GE2 - GigE (eth2)** dropdown.

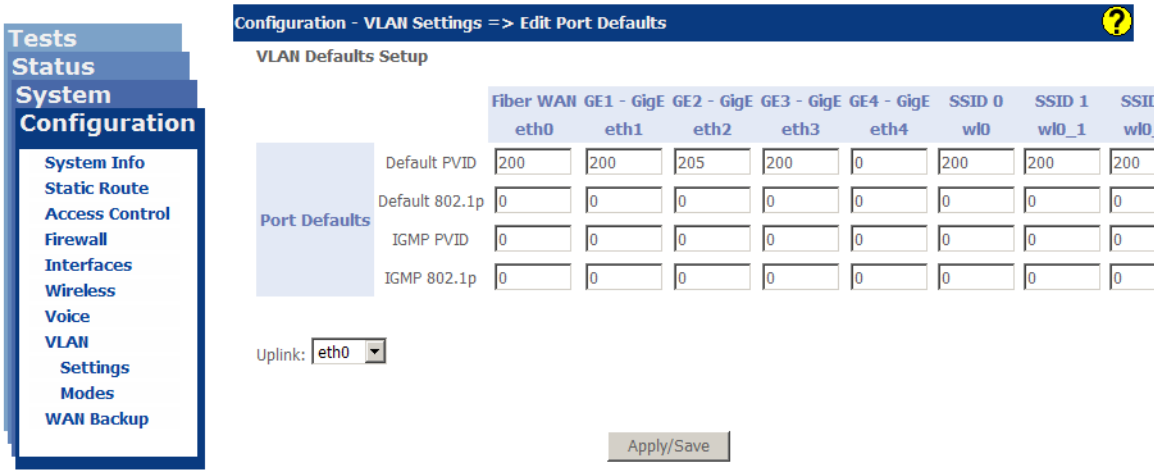
For Dual Managed connections that map to the VEIP select "O" for the uplink port member.

b Click **Save/Apply**

c From the **VLAN | Settings** page click **Edit Port Defaults**

d In the **PVID** text box for **GE2 - GigE eth2**, enter 205 (the same as the ID for the VLAN)

Figure 134: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN	GE1 - GigE	GE2 - GigE	GE3 - GigE	GE4 - GigE	SSID 0	SSID 1	SSII
		eth0	eth1	eth2	eth3	eth4	wl0	wl0_1	wl0_
Port Defaults	Default PVID	200	200	205	200	0	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

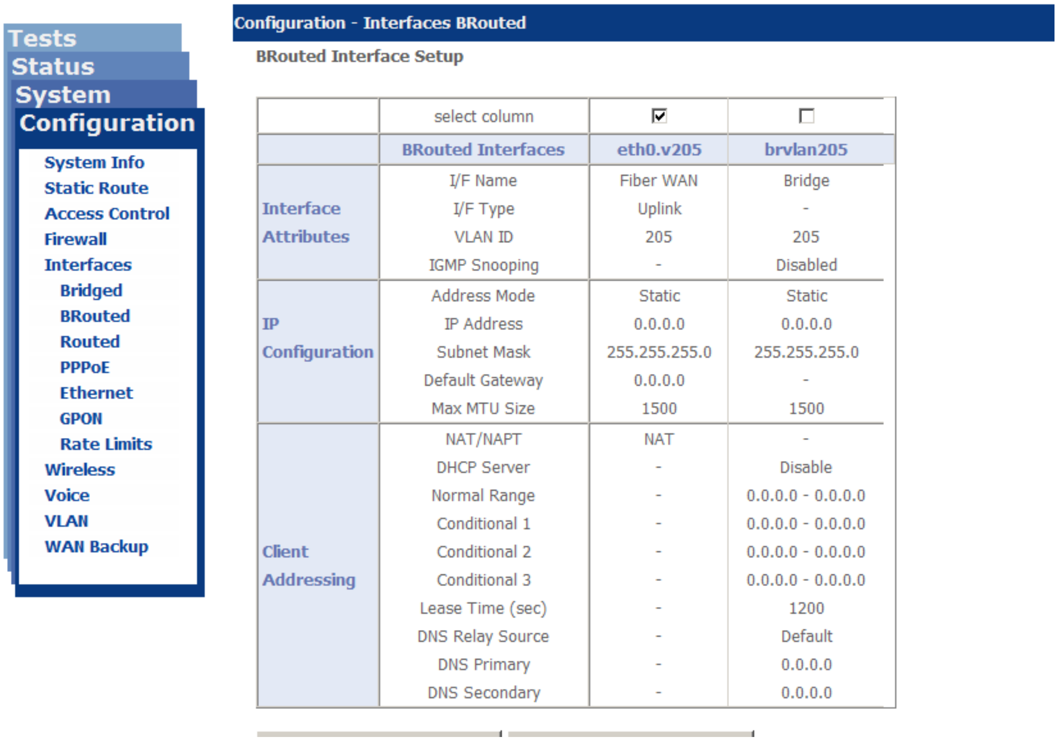
f Click **Save/Apply**

3 Adjust WAN settings

First we will set the addressing for the zNID on the upstream interface. Then we will set the NAT and DNS relay options for downstream devices.

a From the **Interfaces | Routed** page enter a check in the select column for eth0.v402, then click **Edit Selected Interface**

Figure 135: Selecting the fiber WAN interface for the VLAN



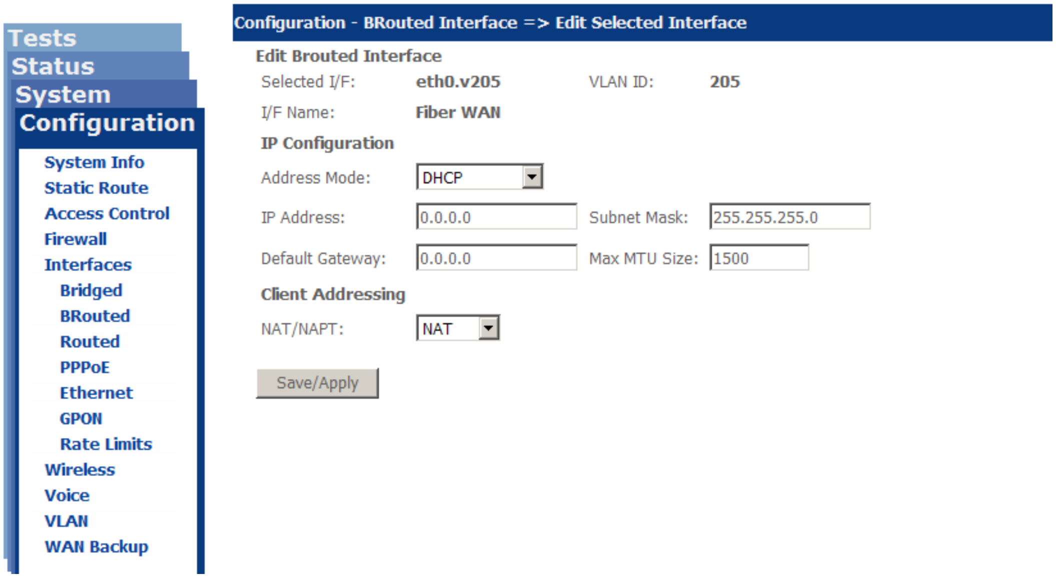
Configuration - Interfaces BRouted

BRouted Interface Setup

	select column	☑	□
	BRouted Interfaces	eth0.v205	brvlan205
Interface Attributes	I/F Name	Fiber WAN	Bridge
	I/F Type	Uplink	-
	VLAN ID	205	205
	IGMP Snooping	-	Disabled
IP Configuration	Address Mode	Static	Static
	IP Address	0.0.0.0	0.0.0.0
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	NAT	-
	DHCP Server	-	Disable
	Normal Range	-	0.0.0.0 - 0.0.0.0
	Conditional 1	-	0.0.0.0 - 0.0.0.0
	Conditional 2	-	0.0.0.0 - 0.0.0.0
	Conditional 3	-	0.0.0.0 - 0.0.0.0
	Lease Time (sec)	-	1200
	DNS Relay Source	-	Default
	DNS Primary	-	0.0.0.0
	DNS Secondary	-	0.0.0.0

b In the **Configuration - Routed Interface --> Edit Selected Interface** page from the IP Configuration section **Address Mode** dropdown select **DHCP**.

Figure 136: Adjusting WAN settings: device addressing and NAT and DNS relay for clients



Configuration - BRouted Interface => Edit Selected Interface

Edit Brouted Interface

Selected I/F: eth0.v205 VLAN ID: 205

I/F Name: Fiber WAN

IP Configuration

Address Mode: DHCP

IP Address: 0.0.0.0 Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0 Max MTU Size: 1500

Client Addressing

NAT/NAPT: NAT

For this example the ZNID will be getting its address from an upstream DHCP server.

Other options for device addressing:

- To assign a permanent IP to the zNID, select **Static** from the **Address Mode** dropdown

  You will need to get the **IP Address** from your ISP as well as the **Subnet Mask**, **Default Gateway** address and **DNS**.

- **Unconfigured**

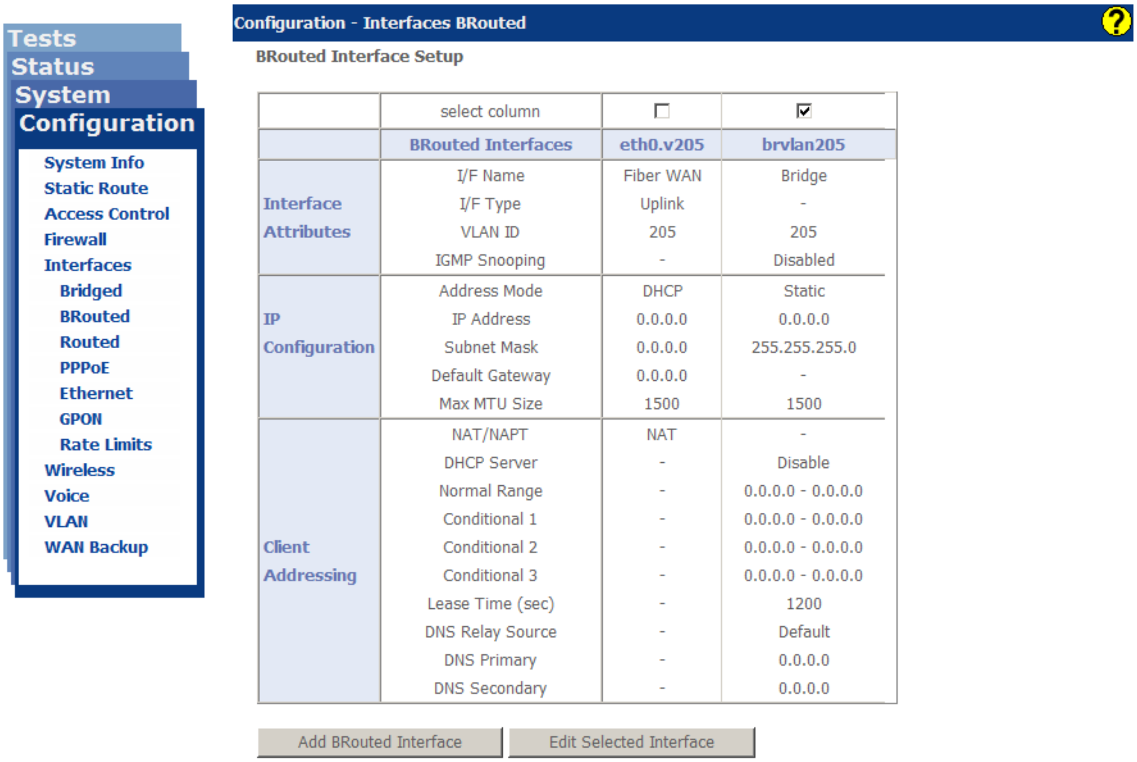
c From the **NAT/NAPT** dropdown select **NAT**

For this example we are going to have private addresses for the downstream devices using Network Address Translation/ Network Address and Port Translation.

4 Adjust LAN settings

a From the **Interfaces | Routed** page enter a check in the select column for eth2.v402, then click **Edit Selected Interface**

Figure 137: Selecting the LAN interface for the VLAN



Configuration - Interfaces BRouted

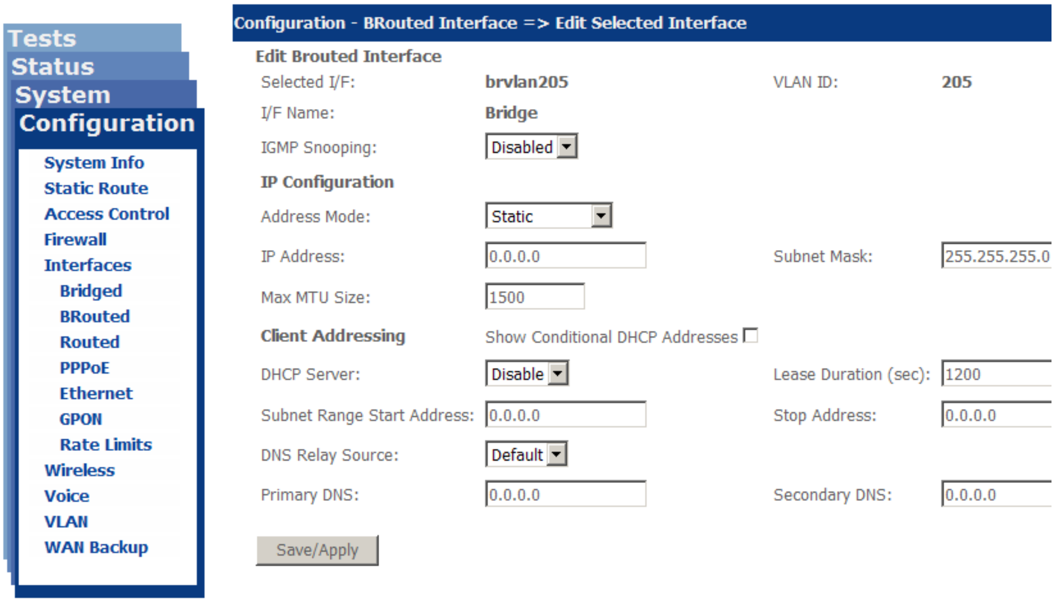
BRouted Interface Setup

	select column	☐	☑
	BRouted Interfaces	eth0.v205	brvlan205
Interface Attributes	I/F Name	Fiber WAN	Bridge
	I/F Type	Uplink	-
	VLAN ID	205	205
	IGMP Snooping	-	Disabled
IP Configuration	Address Mode	DHCP	Static
	IP Address	0.0.0.0	0.0.0.0
	Subnet Mask	0.0.0.0	255.255.255.0
	Default Gateway	0.0.0.0	-
	Max MTU Size	1500	1500
Client Addressing	NAT/NAPT	NAT	-
	DHCP Server	-	Disable
	Normal Range	-	0.0.0.0 - 0.0.0.0
	Conditional 1	-	0.0.0.0 - 0.0.0.0
	Conditional 2	-	0.0.0.0 - 0.0.0.0
	Conditional 3	-	0.0.0.0 - 0.0.0.0
	Lease Time (sec)	-	1200
	DNS Relay Source	-	Default
	DNS Primary	-	0.0.0.0
	DNS Secondary	-	0.0.0.0

b From the **Configuration - Routed Interface => Edit Selected Interface** page, select **Static** from the Address Mode dropdown below **IP Configuration**

For this example we are defining the IP address for the downstream interface, by selecting **Static**.

Figure 138: Selecting the fiber WAN interface for the VLAN



Configuration - BRouted Interface => Edit Selected Interface

Edit Brouted Interface

Selected I/F:	brvlan205	VLAN ID:	205
I/F Name:	Bridge		
IGMP Snooping:	Disabled		
IP Configuration			
Address Mode:	Static		
IP Address:	0.0.0.0	Subnet Mask:	255.255.255.0
Max MTU Size:	1500		
Client Addressing	Show Conditional DHCP Addresses □		
DHCP Server:	Disable	Lease Duration (sec):	1200
Subnet Range Start Address:	0.0.0.0	Stop Address:	0.0.0.0
DNS Relay Source:	Default		
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0

The other options are

- DHCP
- Unconfigured

c From the **DNS Relay Source** dropdown leave **Default**

For this example we are selecting **Default**

A DNS (Dynamic Name System) server provides the translation from a public IP address upstream of the zNID to the private IP address downstream from the zNID.

When set to **Default**, the DNS IP addresses acquired by the WAN uplink interface (via DHCP client or PPPoE client) will be passed down to the LAN side clients as part of the DHCP Offer. This option is not valid if the WAN uplink IP is statically configured, because in that case there are no DNS IPs acquired.

- Static

  When set to **Static**, the DNS IP Addresses that will be passed down to LAN side clients as part of the DHCP Offer must be statically configured.

  The IP address for the DNS relay sources are given in the **Primary DNS** and **Secondary DNS** text boxes.

- Proxy

  When set to **Proxy**, all DNS Requests are sent to the zNID's LAN-side IP Address, and the zNID uses its Local Host Table and its System DNS Client to resolve all DNS requests. The zNID's LAN-side IP Address will be provided as the DNS IP Address to the LAN-side clients in the DHCP Offer. In this case, the Gateway Router IP and the DNS Server IP address will be the same.

5 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

Creating PPPoE tunnels

PPPoE is defined for the uplink port of a VLAN.   In this mode, the zNID 24xx will establish a PPPoE session with a server on behalf of the client connected to the configured port. Each VLAN can have 1 PPPoE session.

The configuration of the PPPoE session requires only a few parameters:

- user name
- password
- authentication method

When in the PPPoE mode, the uplink port will always perform the NAT function. This means that the LAN portion will also have the DHCP server enabled. Depending on how the LAN ports need to be configured, the PPPoE connection will be defined to be either Bridged or Routed.

The zNID 24xx supports PAP, CHAP or MS CHAP. The zNID 24xx can be set to “auto” in which case it will use what ever method the server uses.

- **PPPoE Bridged Mode**

  In PPPoE Bridged Mode mode, a single DHCP server will provide addresses for the devices connected to any of the LAN ports. All ports will be members of the same IP subnet. They are also all members of the same VLAN.

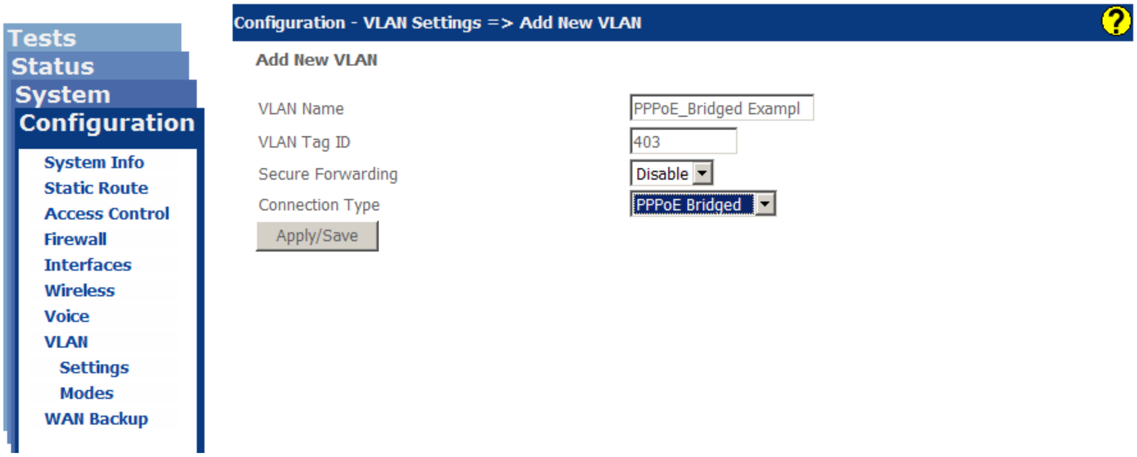
- **PPPoE Routed Mode**

  In PPPoE Routed Mode mode, there is a DHCP server for each LAN port. Each port is on a different IP subnet. This method should be used when the ports are connected to different customers, such as different apartments that are served from a single zNID 24xx.

PPPoE Bridged

1 Create VLAN

Figure 139: Creating a PPPoE bridged VLAN



Add New VLAN

VLAN Name	PPPoE_Bridged Exampl
VLAN Tag ID	403
Secure Forwarding	Disable
Connection Type	PPPoE Bridged

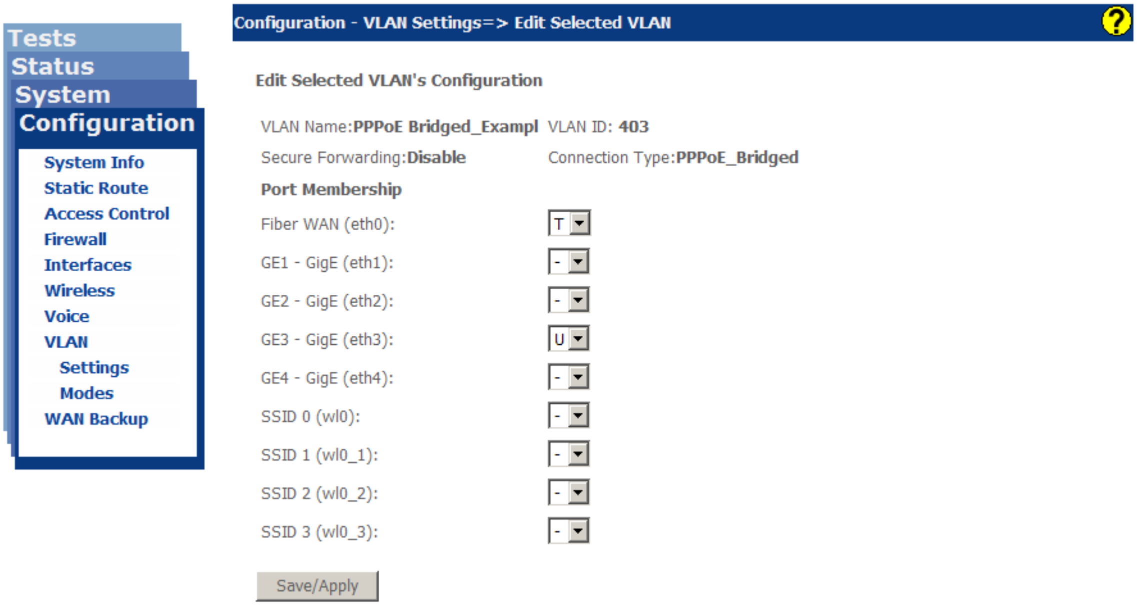
- **a** On the **Configuration|VLAN Settings** page, click **Add New VLAN**
- **b** In the **VLAN Name** text box enter a name for the VLAN
- **c** In the **VLAN Tag ID** text box enter a VLAN ID
- **d** <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

  See *Add New VLAN* on page 148 for more information
- **e** From the **Connection Type** dropdown select **PPPoE Bridged**
- **f** Click **Apply/Save**

2 Select ports and set port defaults

- **a** From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 140: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:PPPoE Bridged_Exampl VLAN ID: 403

Secure Forwarding:Disable Connection Type:PPPoE_Bridged

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	-
GE3 - GigE (eth3):	U
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Save/Apply

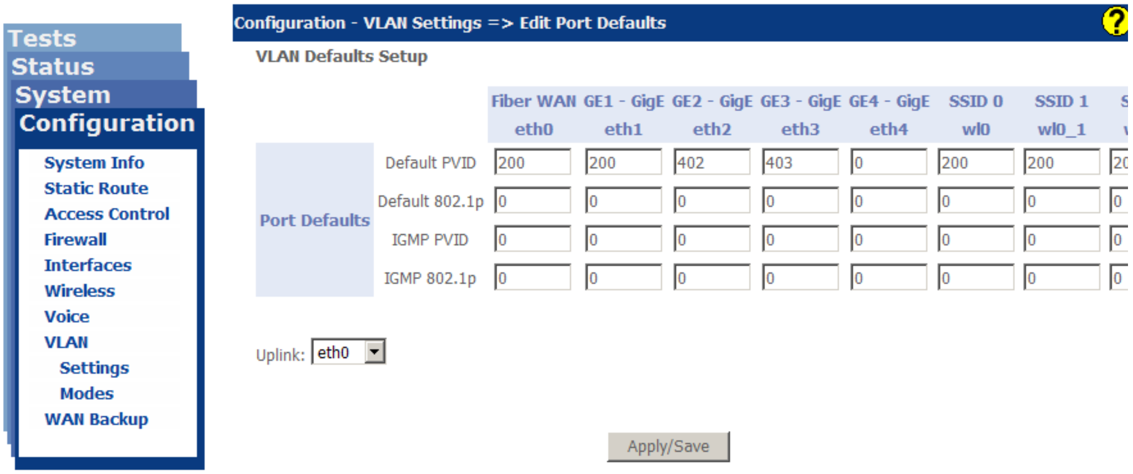
Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown.

In this example we are only selected one untagged downstream interface. Select **U** from the **GE2 - GigE (eth2)** dropdown.

For Dual Managed connections that map to the VEIP select “O” for the uplink port member.

- **b** Click **Save/Apply**
- **c** From the **VLAN | Settings** page click **Edit Port Defaults**
- **d** In the **PVID** text box for **GE2 - GigE eth3**, enter 403 (the same as the ID for the VLAN)

Figure 141: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN	GE1 - GigE	GE2 - GigE	GE3 - GigE	GE4 - GigE	SSID 0	SSID 1	S
		eth0	eth1	eth2	eth3	eth4	wl0	wl0_1	w
Port Defaults	Default PVID	200	200	402	403	0	200	200	20
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

f Click **Save/Apply**

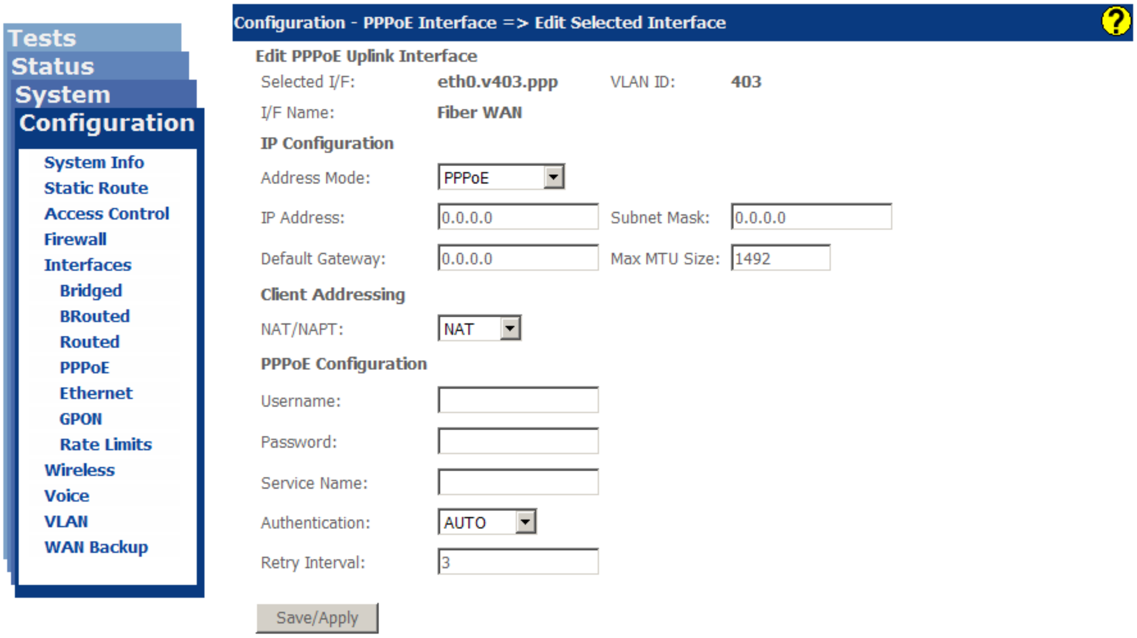
3 Adjust WAN settings

For PPPoE connections the default settings are automatically configured for the WAN interface.

a From the **Interfaces | PPPoE** page enter a check in the select column for eth0.v403, then click **Edit Selected Interface**

b In the **Configuration - Routed Interface --> Edit Selected Interface** page from the IP Configuration section **Address Mode** dropdown **PPPoE** will be set.

Figure 142: For PPPoE you just need to add the username, password and authentication type



Configuration - PPPoE Interface => Edit Selected Interface

Edit PPPoE Uplink Interface

Selected I/F: eth0.v403.ppp VLAN ID: 403

I/F Name: Fiber WAN

IP Configuration

Address Mode: PPPoE

IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 Max MTU Size: 1492

Client Addressing

NAT/NAPT: NAT

PPPoE Configuration

Username:

Password:

Service Name:

Authentication: AUTO

Retry Interval: 3

For PPPoE the device addressing mode is PPPoE by default.

c In the **NAT/NAPT** dropdown below Client Addressing **Enable** will be selected

For PPPoE NAT/NAPT is enabled by default.

d In the **DNS Relay Source** dropdown **PPPoE** is selected.

For PPPoE the DNS relay source is set to PPPoE by default.

e Set the PPP username, password and authentication method

In the Username, Password, Service Name and Retry Interval text boxes enter the information supplied by your ISP.

In the **Authentication** dropdown select **Auto**, or the option requested by your ISP.

4 Adjust LAN settings

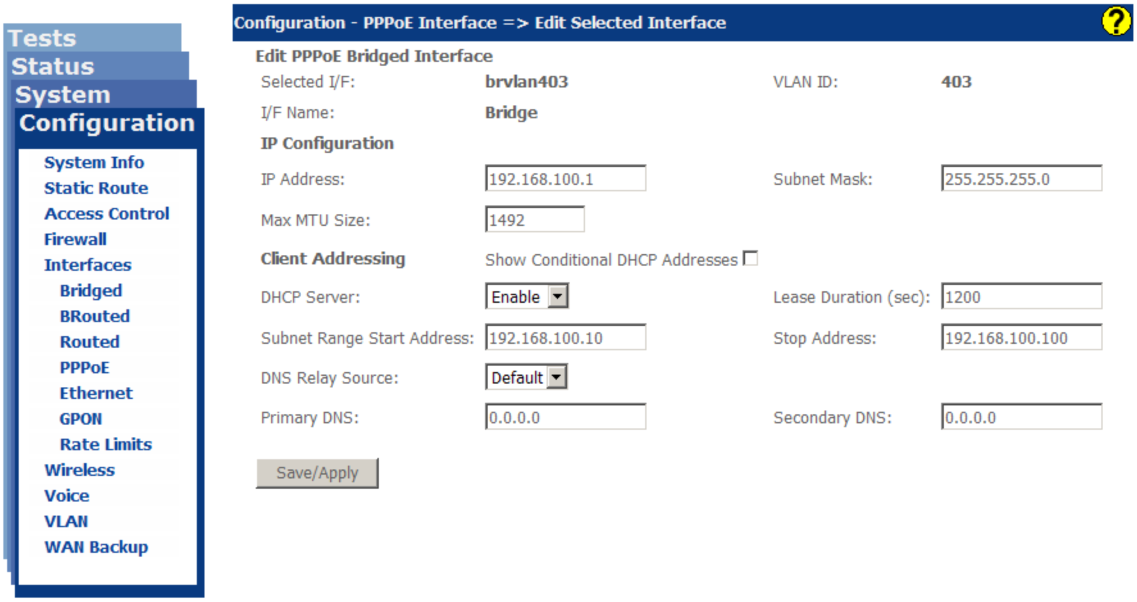
For PPPoE connections the LAN side you define the IP address of the interface and the subnet using DHCP (by default).

a From the **Interfaces | Routed** page enter a check in the select column for eth3.v403, then click **Edit Selected Interface**

b In the **IP Address** text box below **IP Configuration** enter an IP address (192.168.100.1) and in the **Subnet Mask** define the mask for the subnet (255.255.255.0)

c From the **DHCP Server** dropdown below Client Addressing select Enable.

Figure 143: Defining the subnet for the PPPoE bridged VLAN



Configuration - PPPoE Interface => Edit Selected Interface

Edit PPPoE Bridged Interface

Selected I/F:	brvlan403	VLAN ID:	403
I/F Name:	Bridge		
IP Configuration			
IP Address:	192.168.100.1	Subnet Mask:	255.255.255.0
Max MTU Size:	1492		
Client Addressing	Show Conditional DHCP Addresses □		
DHCP Server:	Enable	Lease Duration (sec):	1200
Subnet Range Start Address:	192.168.100.10	Stop Address:	192.168.100.100
DNS Relay Source:	Default		
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0

d In the **Subnet Range Start Address** text box enter a start address for the subnet (192.168.100.10)

e In the **Stop Address** text box enter an ending address for the subnet range (192.168.100.100)

f In the **Lease Duration (sec)** text box enter 86400.

86400 is 24 hours (in seconds, 60 x 60 x 24)

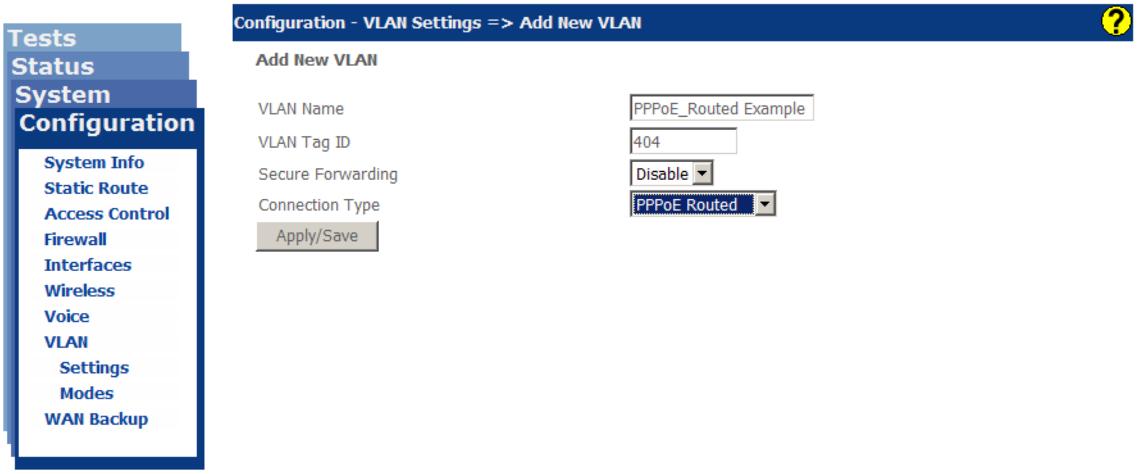
5 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

PPPoE Routed

1 Create VLAN

Figure 144: Creating a PPPoE routed VLAN



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name	PPPoE_Routed Example
VLAN Tag ID	404
Secure Forwarding	Disable
Connection Type	PPPoE Routed

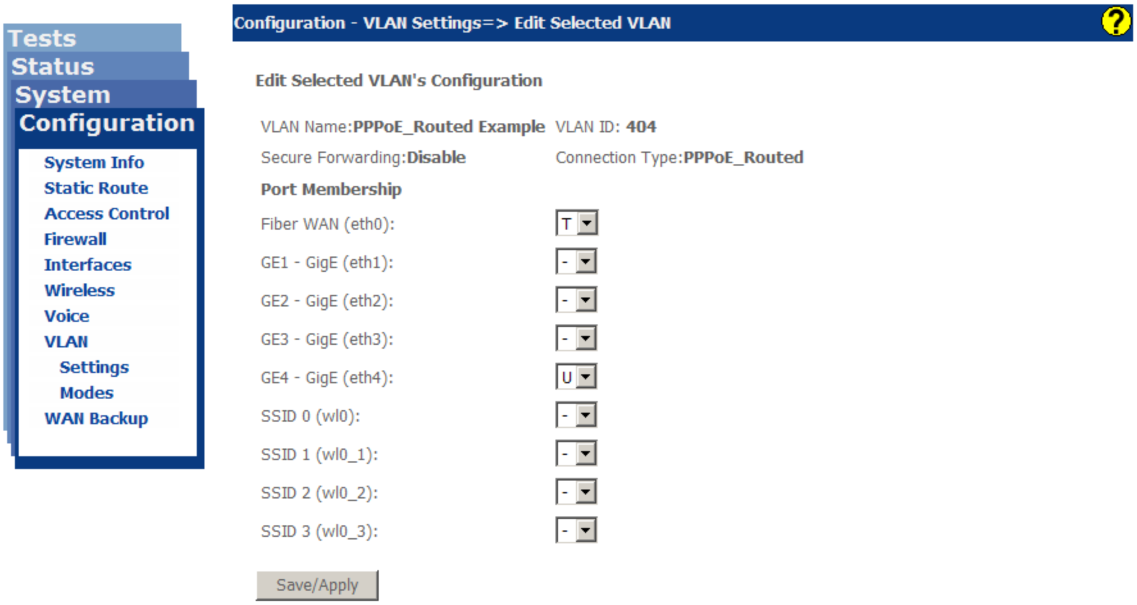
- **a** On the **Configuration|VLAN Settings** page, click **Add New VLAN**
- **b** In the **VLAN Name** text box enter a name for the VLAN
- **c** In the **VLAN Tag ID** text box enter a VLAN ID
- **d** <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

  See *Add New VLAN* on page 148 for more information
- **e** From the **Connection Type** dropdown select **PPPoE Routed**
- **f** Click **Apply/Save**

2 Select ports and set port defaults

- **a** From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 145: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**PPPoE_Routed Example** VLAN ID: **404**

Secure Forwarding:**Disable** Connection Type:**PPPoE_Routed**

Port Membership

Fiber WAN (eth0):	T
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	-
GE3 - GigE (eth3):	-
GE4 - GigE (eth4):	U
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown.

In this example we are only selected one untagged downstream interface. Select **U** from the **GE4 - GigE (eth4)** dropdown.

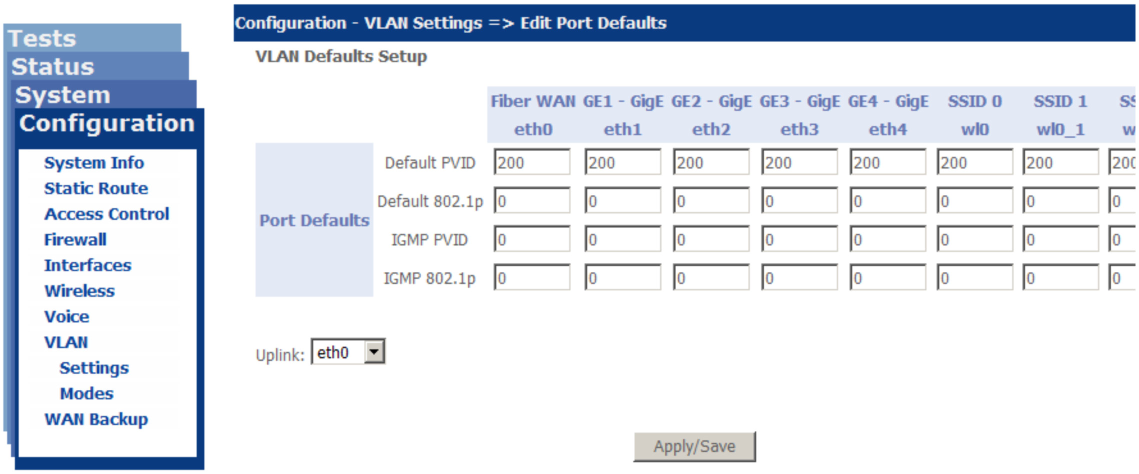
For Dual Managed connections that map to the VEIP select “O” for the uplink port member.

b Click **Save/Apply**

c From the **VLAN | Settings** page click **Edit Port Defaults**

d In the **PVID** text box for **GE4 - GigE eth4**, enter 404 (the same as the ID for the VLAN)

Figure 146: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SS w
Port Defaults	Default PVID	200	200	200	200	200	200	200	20(
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

f Click **Save/Apply**

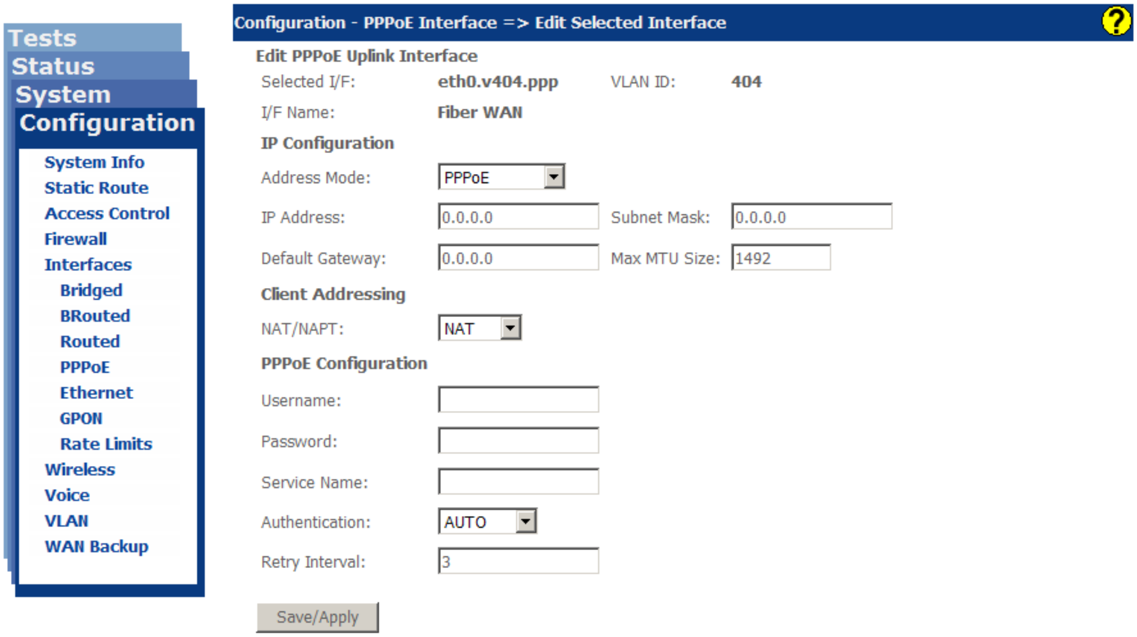
3 Adjust WAN settings

For PPPoE connections the default settings are automatically configured for the WAN interface.

a From the **Interfaces | PPPoE** page enter a check in the select column for eth0.v404, then click **Edit Selected Interface**

b In the **Configuration - Routed Interface --> Edit Selected Interface** page from the IP Configuration section **Address Mode** dropdown **PPPoE** will be set.

Figure 147: For PPPoE you just need to add the username, password and authentication type



Configuration - PPPoE Interface => Edit Selected Interface

Edit PPPoE Uplink Interface

Selected I/F: eth0.v404.ppp VLAN ID: 404

I/F Name: Fiber WAN

IP Configuration

Address Mode: PPPoE

IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 Max MTU Size: 1492

Client Addressing

NAT/NAPT: NAT

PPPoE Configuration

Username:

Password:

Service Name:

Authentication: AUTO

Retry Interval: 3

For PPPoE the device addressing mode is PPPoE by default.

c In the **NAT/NAPT** dropdown below **Client Addressing, NAT** will be selected

For PPPoE NAT is selected by default.

d Set the PPP username, password and authentication method

In the **Username**, **Password**, **Service Name** and **Retry Interval** text boxes enter the information supplied by your ISP.

In the **Authentication** dropdown select **Auto**, or the option requested by your ISP.

4 Adjust LAN settings

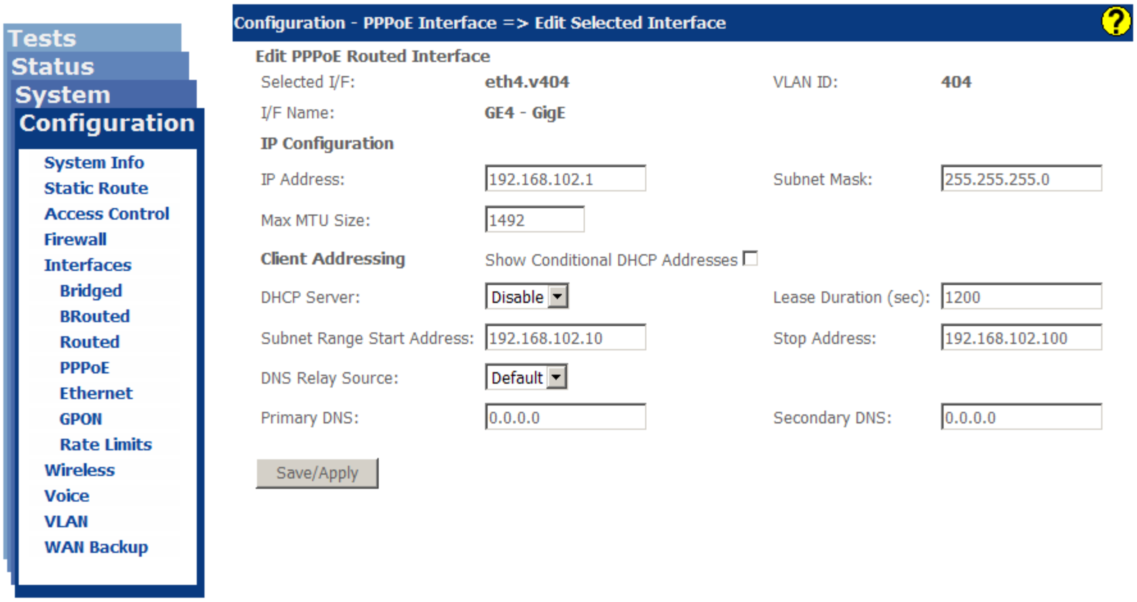
For PPPoE connections the LAN side you define the IP address of the interface and the subnet using DHCP (by default).

a From the **Interfaces | PPPoE** page enter a check in the select column for eth4.v404, then click **Edit Selected Interface**

b In the **IP Address** text box below **IP Configuration** enter an IP address (192.168.102.1) and in the **Subnet Mask** define the mask for the subnet (255.255.255.0)

c From the **DHCP Server** dropdown below **Client Addressing** select **Enable**.

Figure 148: Defining the subnet for the PPPoE bridged VLAN



Configuration - PPPoE Interface => Edit Selected Interface

Edit PPPoE Routed Interface

Selected I/F:	eth4.v404	VLAN ID:	404
I/F Name:	GE4 - GigE		
IP Configuration			
IP Address:	192.168.102.1	Subnet Mask:	255.255.255.0
Max MTU Size:	1492		
Client Addressing	Show Conditional DHCP Addresses □		
DHCP Server:	Disable	Lease Duration (sec):	1200
Subnet Range Start Address:	192.168.102.10	Stop Address:	192.168.102.100
DNS Relay Source:	Default		
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0

Save/Apply

d In the **Subnet Range Start Address** text box enter a start address for the subnet (192.168.102.10)

e In the **Stop Address** text box enter an ending address for the subnet range (192.168.102.100)

f In the **Lease Duration (sec)** text box enter 86400.

86400 is 24 hours (in seconds, 60 x 60 x 24)

5 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

Creating wireless connections

Wireless connections are created just like other connections in that the wireless interface is selected for port membership

Creating a new VLAN with wireless connection

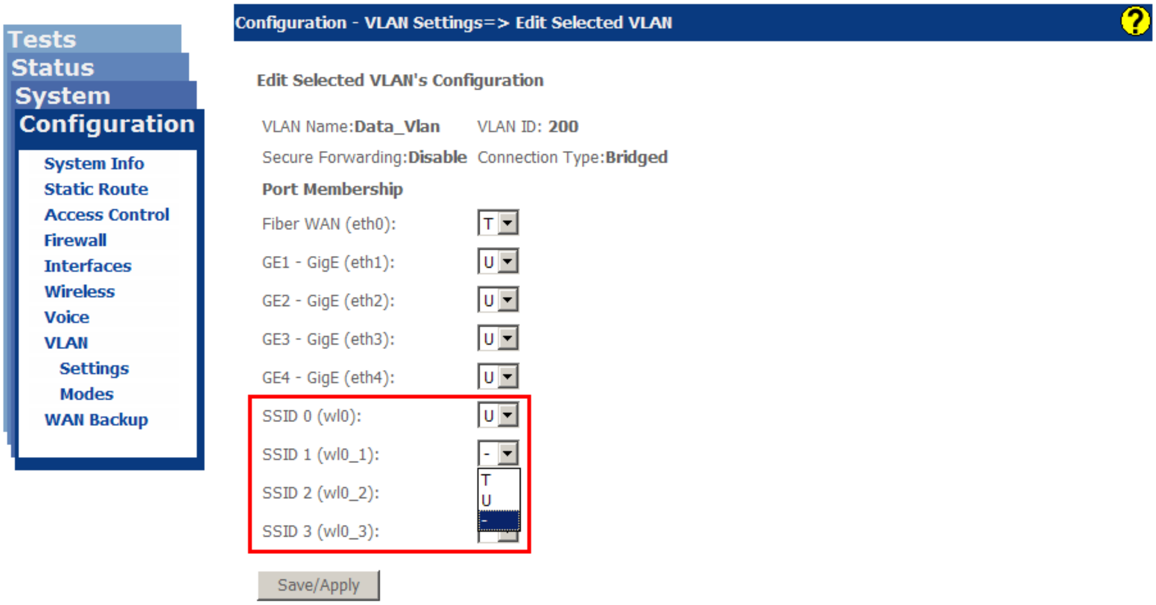
1 Create VLAN

Follow the steps for the type of connection: bridged, routed, PPPoE bridged or PPPoE routed

2 Select ports and set port defaults

Follow the steps for the type of connection: bridged, routed, PPPoE bridged or PPPoE routed and include the wireless ports in the port

Figure 149: Port membership for wireless interfaces



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**Data_Vlan** VLAN ID: **200**

Secure Forwarding:**Disable** Connection Type:**Bridged**

Port Membership

Fiber WAN (eth0): T
GE1 - GigE (eth1): U
GE2 - GigE (eth2): U
GE3 - GigE (eth3): U
GE4 - GigE (eth4): U
SSID 0 (wl0): U
SSID 1 (wl0_1): -
SSID 2 (wl0_2): T
SSID 3 (wl0_3): U
-

Save/Apply

3 Adjust WAN settings (Routed and PPPoE connections)

Follow the steps for the type of connection: bridged, routed, PPPoE bridged or PPPoE routed

4 Adjust LAN settings (Routed and PPPoE connections)

Follow the steps for the type of connection: bridged, routed, PPPoE bridged or PPPoE routed

5 Configure Wireless (Wireless connections only)

Set authentication and encryption features as well as other wireless options. See Wireless, page 108 for the wireless options.

Adding a wireless interface to an existing VLAN

1. In the navigation pane select **Configuration | VLAN | Settings**
2. On the **Configuration - VLAN Settings** page, put a check in the checkbox for the VLAN which you wish to add the wireless interface, then click **Edit Selected VLAN**
3. On the **Configuration - VLAN Settings => Edit Selected VLAN** page, select **U** or **T** from the dropdown associated with the wireless interface

   U and **T** are for untagged or tagged, usually **U** for downstream interfaces such as wireless.

Creating video connections

IGMP snooping may be set on bridged or brouted VLANs.

To add IGMP snooping to a bridged VLAN:

1 Create VLAN

  a In the **VLAN Name** text box enter a name for the VLAN

  b In the **VLAN Tag ID** text box enter a VLAN ID

  c <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

  d From the **Connection Type** dropdown select **Bridged**

  e Click **Apply/Save**

2 Select ports and set port defaults

  a From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

  Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown

  In this example we are only selected one untagged downstream interface. Select **U** from the **GE1 - GigE (eth1)** dropdown

  b Click **Save/Apply**

  c From the **VLAN | Settings** page click **Edit Port Defaults**

  d In the **PVID** text box for **GE1 - GigE eth1**, enter 401 (the same as the ID for the VLAN)

  e From the **Uplink** eth0 should be selected

  Selecting the Fiber WAN interface adds this VLAN to the uplink.

  f Click **Save/Apply**

3 Set the bridged interface for IGMP

  a Select **Configuration|Interfaces|Bridged**

  b In the checkbox for the VLAN enter a check and click **Edit Selected Interface**.

  c From the I**GMP Snooping** dropdown select Enabled

  d Click **Save/Apply**

Creating voice connections

Voice connections require that the proper version of the software is loaded onto the zNID. SIP and SIP-PLAR versions are S versions, such as **S**2.4.112. MGCP versions are M versions, such as **M**2.4.112.

If you do not have the proper version of the software consult your Zhone representative.

To load the upload the software onto the zNID, see *Update software* on page 55.

SIP

1 The SIP version of the software must be loaded on the zNID

See Update software, page 55

2 Create the voice VLAN

Select **Bridged** for the **Connection Type**.

3 Bind the POTS interface to the VLAN

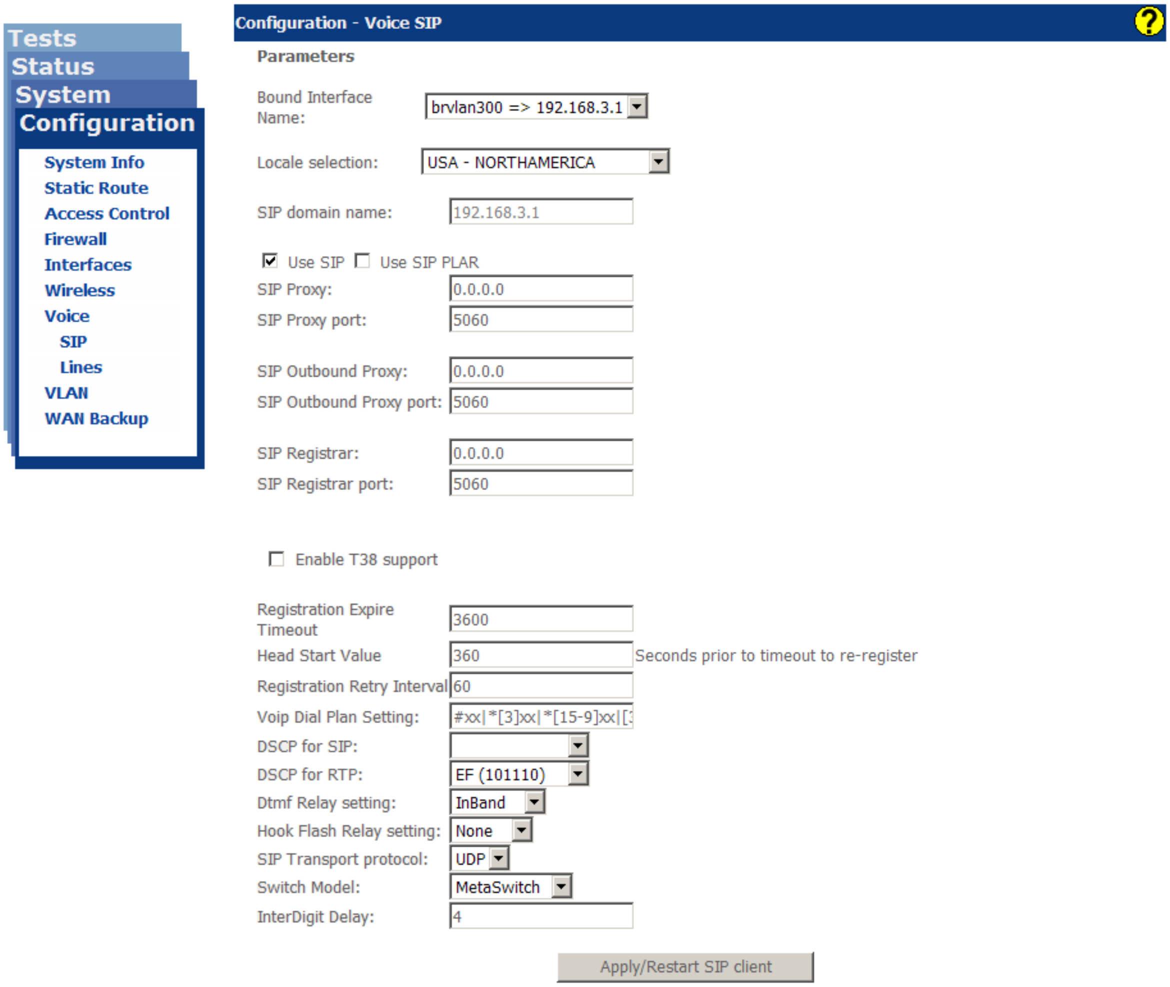
a Select **Configuration|Voice|SIP**

b From the **Bound Interface Name** dropdown, select the VLAN created for voice.

4 Configure SIP

See *SIP* on page 135 for a description of the configuration parameters

Figure 150: The SIP configuration screen



Configuration - Voice SIP

Parameters

Bound Interface Name: brvlan300 => 192.168.3.1

Locale selection: USA - NORTHAMERICA

SIP domain name: 192.168.3.1

☑ Use SIP ☐ Use SIP PLAR

SIP Proxy: 0.0.0.0

SIP Proxy port: 5060

SIP Outbound Proxy: 0.0.0.0

SIP Outbound Proxy port: 5060

SIP Registrar: 0.0.0.0

SIP Registrar port: 5060

☐ Enable T38 support

Registration Expire Timeout: 3600

Head Start Value: 360 Seconds prior to timeout to re-register

Registration Retry Interval: 60

Voip Dial Plan Setting: #xx|*[3]xx|*[15-9]xx|[3

DSCP for SIP:

DSCP for RTP: EF (101110)

Dtmf Relay setting: InBand

Hook Flash Relay setting: None

SIP Transport protocol: UDP

Switch Model: MetaSwitch

InterDigit Delay: 4

5 Select Admin State and define....

6 Configure line settings....

7 Click **Apply/Restart SIP client**

SIP-PLAR

1 The SIP version of the software must be loaded on the zNID (includes SIP PLAR

See Update software, page 55

2 Create the voice VLAN

Select **Bridged** for the **Connection Type**.

3 Bind the POTS interface to the VLAN

a Select **Configuration|Voice|SIP**

b From the **Bound Interface Name** dropdown, select the VLAN created for voice.

4 Configure SIP-PLAR

See *SIP-PLAR* on page 136 for a description of the configuration parameters

5 Select Admin State and define....

6 Configure line settings....

7 Click **Apply/Restart SIP client**

MGCP

1 The MGCP version of the software must be loaded on the zNID

See Update software, page 55

2 Create the voice VLAN

Select **Bridged** for the **Connection Type**.

3 Bind the POTS interface to the VLAN

a Select **Configuration|Voice|MGCP**

b From the **Bound Interface Name** dropdown, select the VLAN created for voice.

4 Configure MGCP

See *MGCP* on page 139 for a description of the configuration parameters

5 Select Admin State and define....

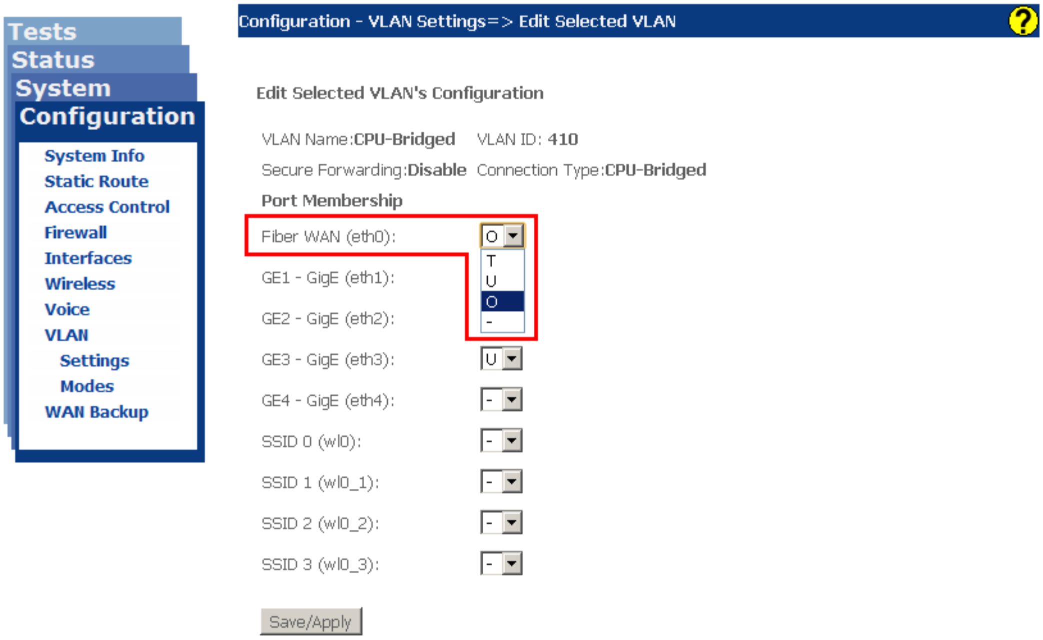
6 Configure line settings....

7 Click **Apply/Restart SIP client**

Creating Dual Managed connections

Dual Managed connections using the virtual UNI (VEIP) between the RG and OMCI are created in the same manner as other connections. The only difference is that in the port selection process, rather than select “T” (for tagged) or “U” (for untagged) for the uplink, you select “O” (for OMCI).

Figure 151:



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**CPU-Bridged** VLAN ID: **410**

Secure Forwarding:**Disable** Connection Type:**CPU-Bridged**

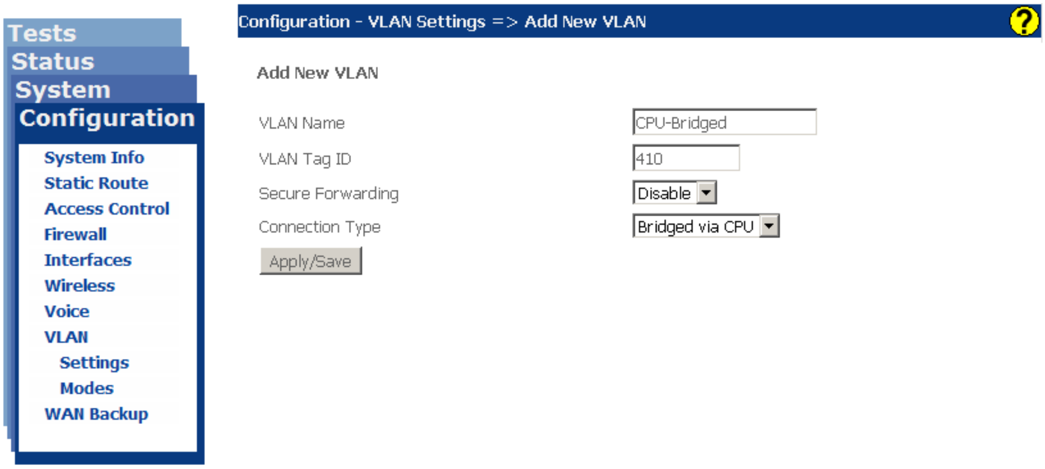
Port Membership

Fiber WAN (eth0):	O
GE1 - GigE (eth1):	
GE2 - GigE (eth2):	
GE3 - GigE (eth3):	U
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

CPU Bridged for VEIP

1 Create VLAN

Figure 152: Creating a bridged VLAN



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name	CPU-Bridged
VLAN Tag ID	410
Secure Forwarding	Disable
Connection Type	Bridged via CPU

a On the **Configuration|VLAN Settings** page, click **Add New VLAN**

b In the **VLAN Name** text box enter a name for the VLAN

c In the **VLAN Tag ID** text box enter a VLAN ID

d <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

See *Add New VLAN* on page 148 for more information

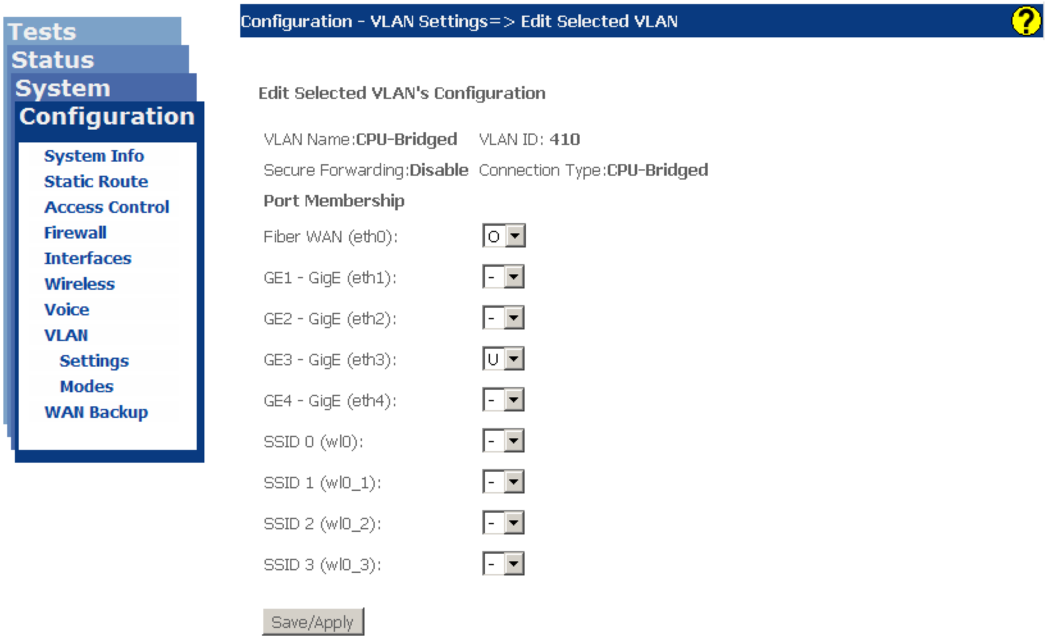
e From the **Connection Type** dropdown select **Bridged**

f Click **Apply/Save**

2 Select ports and set port defaults

a From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

Figure 153: Selecting port members and their tagging



Configuration - VLAN Settings=> Edit Selected VLAN

Edit Selected VLAN's Configuration

VLAN Name:**CPU-Bridged** VLAN ID: **410**

Secure Forwarding:**Disable** Connection Type:**CPU-Bridged**

Port Membership

Fiber WAN (eth0):	O
GE1 - GigE (eth1):	-
GE2 - GigE (eth2):	-
GE3 - GigE (eth3):	U
GE4 - GigE (eth4):	-
SSID 0 (wl0):	-
SSID 1 (wl0_1):	-
SSID 2 (wl0_2):	-
SSID 3 (wl0_3):	-

Normally the uplink **(Fiber WAN (eth0)** will be Tagged as in this example. Select **T** from the **Fiber WAN (eth0)** dropdown

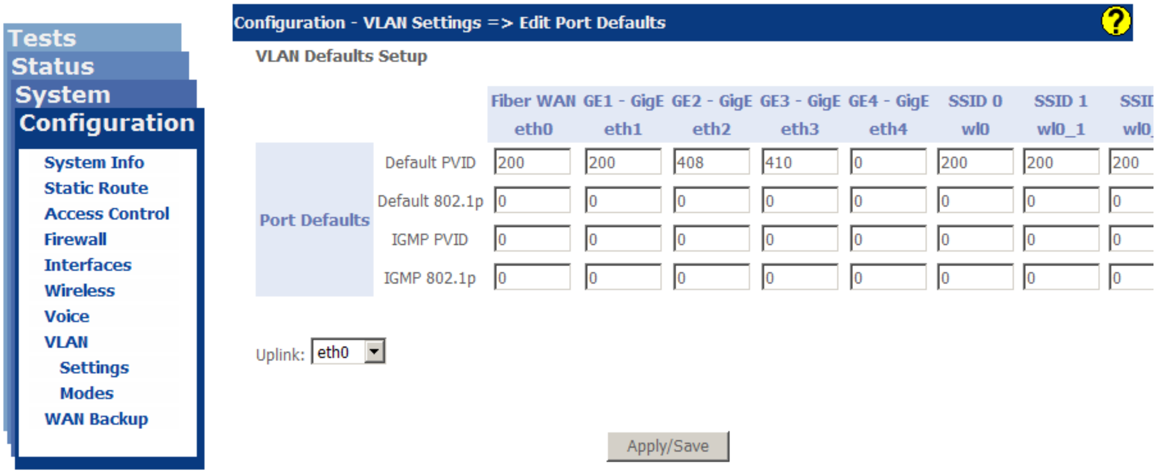
In this example we are only selected one untagged downstream interface. Select **U** from the **GE1 - GigE (eth1)** dropdown

b Click **Save/Apply**

c From the **VLAN | Settings** page click **Edit Port Defaults**

d In the **PVID** text box for **GE1 - GigE eth1**, enter 410 (the same as the ID for the VLAN)

Figure 154: Setting the PVID for the interface



Configuration - VLAN Settings => Edit Port Defaults

VLAN Defaults Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSII wl0_
Port Defaults	Default PVID	200	200	408	410	0	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0

Uplink: eth0

Note: Make sure that a VLAN is created with a matching VLAN ID and the LAN ports are configured as untagged members of that VLAN.

The default PVID is only used to determine how ingress untagged traffic will be tagged. The VLAN table defines the egress action.

e From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

f Click **Save/Apply**

3 Configure Wireless (Wireless connections only)

Set port membership, authentication and encryption features as well as other wireless options. See Creating wireless connections, page 188.

Advanced features

VLANS

The zNID 24xxs support VLAN-based services. This section describes the types of VLANs that are supported on this device. When configured for normal single-tagged mode, all ports are members of a VLAN. They can be untagged or tagged members. Alternatively, ports can be double tagged members of an S-VLAN.

Ethernet frames that are tagged have a VLAN ID and priority as part of the Ethernet frame. In this product that is called the “C” tag or the Customer tag. This family of products also supports the double tagging feature. The outer tag is called the “S-Tag” or the Service Provider tag. This double tag capability is an advanced feature that allows traffic from multiple clients to be sent through the network in a common VLAN.

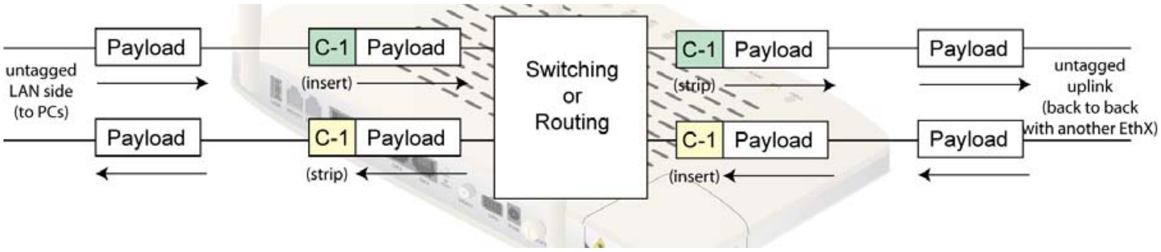
Once the S-Tag mode has been selected from the VLAN Mode page, traffic leaving the port designated as the S-Tag port, will have the outer S-tag added to the frame.

The S-Tag mode only works with ports that been defined as TLS members for the S-LAN, where all tagged traffic on a port is accepted without having to configure each individual VLAN. When this traffic leaves the system, it will have the outer S-tag applied to the packets.

All ports untagged

In some configurations the Ethernet ports appear as untagged ports. The traffic in and out of the ONU will be standard Ethernet frames. However, internally, the Ethernet frames are VLAN tagged (C-1). This allows the ONU to prioritize and forward traffic appropriately. The figure below shows the traffic flow for ports that are untagged.

Figure 155: All ports untagged

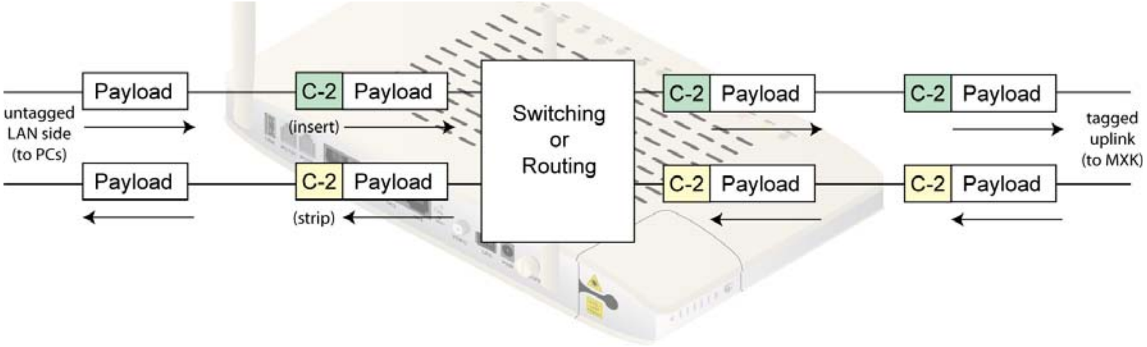


This configuration is valid only when all ports are members of the same VLAN. Otherwise, there is no way to separate traffic. This configuration would not typically be used when the zNID 24xx is connected to an MXK. The MXK expects the traffic to be tagged, as described in the next section.

Tagged uplink port untagged LAN ports

The diagram below shows an example of a VLAN tag (C-2) being added to the Ethernet frame received on the LAN port. In this case the VLAN tag remains on the frame as it is sent to the network, on the port that has been designated as the Uplink port. Typically, this is the fiber port. Traffic that is received from the network is expected to have the C-2 VLAN tag. This tag will be removed before the Ethernet frame is sent to the LAN port.

Figure 156: Tagged uplink, untagged LAN ports

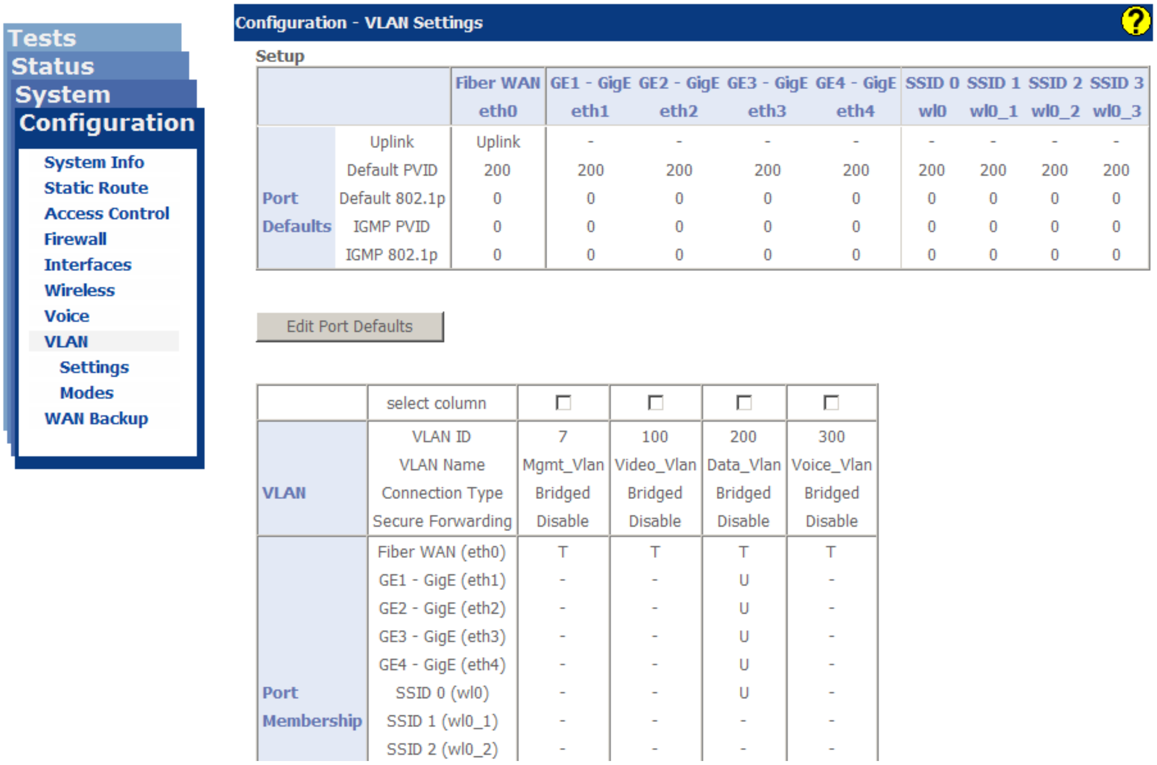


This is the most common configuration of the zNID 24xx. The MXK expects tagged traffic on the uplink, while most PCs and set top boxes only use untagged traffic.

The VLAN configuration web page shows an example of the uplink port being tagged and the LAN ports being untagged. This is the standard configuration when connected to an MXK.

If a tagged frame is received on the LAN port, it will be forwarded upstream unmodified. However, in the downstream direction the VLAN tag will be removed before sending the frame out the LAN port. This could lead to undesirable results, since the device sending tagged frames probably expects to receive tagged frames.

Figure 157: Configuration of VLAN settings



Configuration - VLAN Settings

Setup

		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSID 2 wl0_2	SSID 3 wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	Default PVID	200	200	200	200	200	200	200	200	200
	Default 802.1p	0	0	0	0	0	0	0	0	0
	IGMP PVID	0	0	0	0	0	0	0	0	0
	IGMP 802.1p	0	0	0	0	0	0	0	0	0

Edit Port Defaults

	select column	□	□	□	□
VLAN	VLAN ID	7	100	200	300
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan
	Connection Type	Bridged	Bridged	Bridged	Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable
Port Membership	Fiber WAN (eth0)	T	T	T	T
	GE1 - GigE (eth1)	-	-	U	-
	GE2 - GigE (eth2)	-	-	U	-
	GE3 - GigE (eth3)	-	-	U	-
	GE4 - GigE (eth4)	-	-	U	-
	SSID 0 (wl0)	-	-	U	-
	SSID 1 (wl0_1)	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-

Tagged uplink port and tagged LAN ports

The diagram below shows an example where the traffic is received on the LAN port with a VLAN tag (C-3) already included. In this case the VLAN tag remains on the frame as it is sent to the network on the port that has been designated as the Uplink port. Traffic that is received from the network is expected to have the C-3 VLAN tag. That traffic is prioritized and forwarded based on that VLAN tag. In this case the LAN Ethernet port is tagged, therefore the C-3 VLAN tag is not stripped from the frame before being sent to the LAN port as described in the previous example. In this case, the VLAN tag is preserved.

Figure 158: Tagged uplink and tagged LAN ports

Each Ethernet port can be a member of a different VLAN. The ports can be tagged or untagged. For this example both Ethernet ports are tagged. The web page below shows the configuration for a zNID 24xx that is configured for tagged Ethernet ports and tagged uplink port.

In this mode, if an untagged frame is received on the LAN port, a VLAN tag will be added as defined by the PVID and the frame will be forwarded upstream. In the downstream direction, the tagged frame will be passed to the LAN port without any modifications. This could lead to undesirable results since the device that sent untagged frames probably expects to receive untagged frames.

S-Tagged

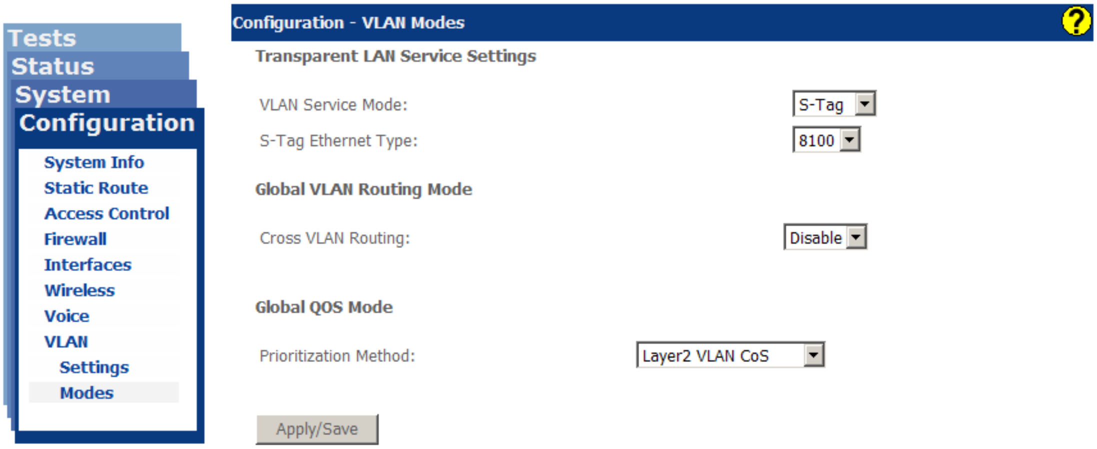
S-Tag or QinQ is a method of adding a second VLAN tag to an Ethernet frame. This can be useful for Service providers that have multiple clients on the same ONU, or for business applications in which the client has their network segmented with multiple private VLANs that may conflict with VLANs in use by other customers of the same service provider. The S-Tag concept allows the service provider to take tagged traffic from a customer network and transport that traffic though through the network on a single VLAN without the traffic from one client interfering with the traffic from another client. The client ports are unaware of the double tag, since it is stripped before the Ethernet frame is sent to the LAN port.

The outer S-tag is identified by a unique Tag Protocol Identifier (TPID). Typical values for the TPID are 88A8, 8100, 9100, 9200, or 9300. The default value is 8100. This family of products allows that field to be specified by the user.

Figure 159: S-Tagged on uplink, tagged LAN

On the web interface, the S-tag feature is defined on the VLAN mode page as shown below. Once enabled, all VLAN traffic being sent upstream will have the outer S-tag applied to the packet.

Figure 160: Stag is set from the VLAN Service Mode dropdown



Configuration - VLAN Modes

Transparent LAN Service Settings

VLAN Service Mode: S-Tag

S-Tag Ethernet Type: 8100

Global VLAN Routing Mode

Cross VLAN Routing: Disable

Global QOS Mode

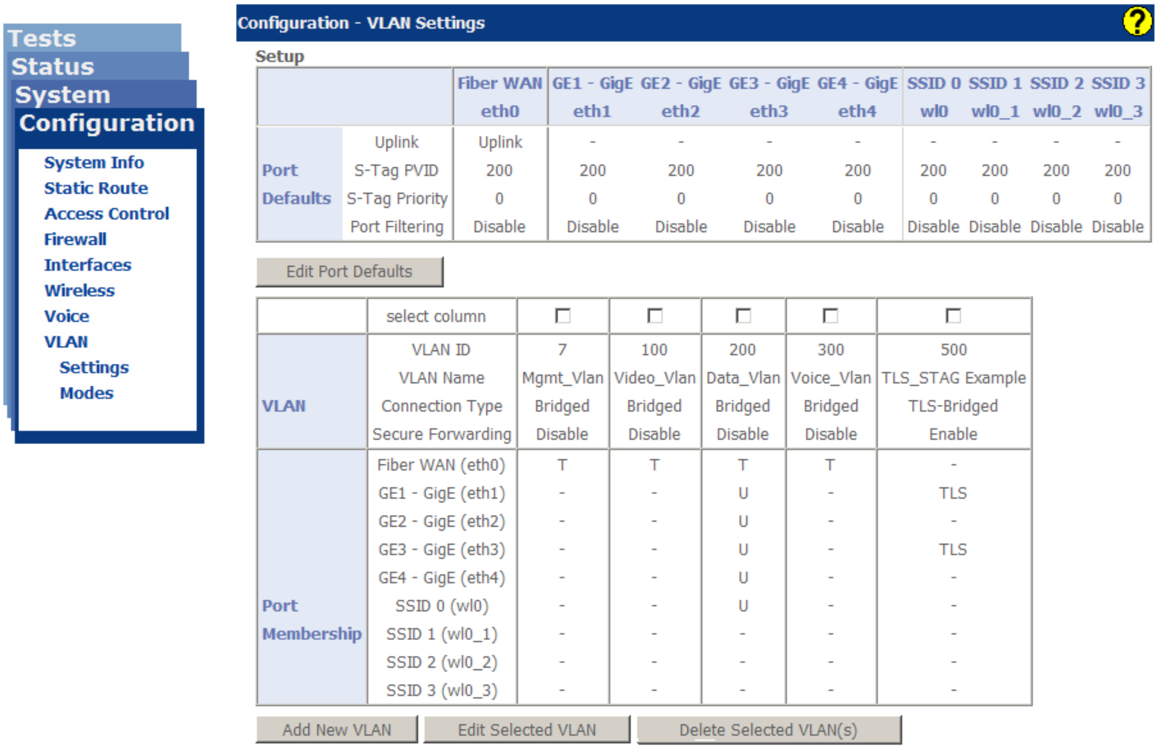
Prioritization Method: Layer2 VLAN CoS

TLS mode

Once the ONU has been set for S-tag mode, individual ports can be configured for TLS (Transparent LAN Services) mode, where all the tagged traffic received on a TLS port is tagged with an outer S-Tag and forward upstream. The web page below shows an example of a configuration that has tagged traffic on both Ethernet ports, and the upstream traffic has an additional S-tag on the packet. In this example, the traffic on each Ethernet port could be from different service providers. The service providers could be using the same VLAN IDs, but the traffic would remain segregated since they have unique S-tag IDs.

Based on the figure below, in this example, port 1 is set to be in TLS mode. In that mode, all of the data received on port 1 will have an outer tag of 101added each packet. Data received on the uplink port is expected to have an outer S-tag of 101, which will be stripped on input.

Figure 161: TLS bridge



Setup

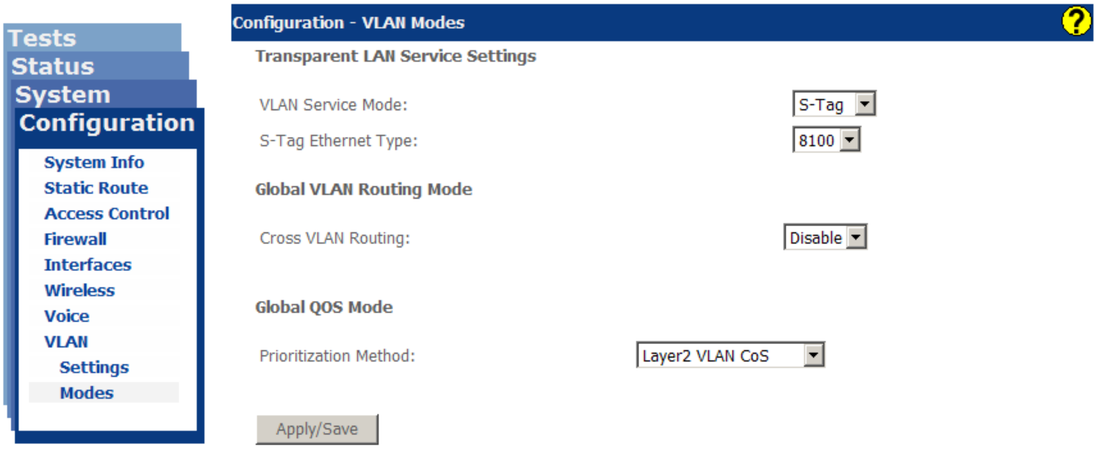
		Fiber WAN eth0	GE1 - GigE eth1	GE2 - GigE eth2	GE3 - GigE eth3	GE4 - GigE eth4	SSID 0 wl0	SSID 1 wl0_1	SSID 2 wl0_2	SSID 3 wl0_3
Port Defaults	Uplink	Uplink	-	-	-	-	-	-	-	-
	S-Tag PVID	200	200	200	200	200	200	200	200	200
	S-Tag Priority	0	0	0	0	0	0	0	0	0
	Port Filtering	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable

	select column	□	□	□	□	□
VLAN	VLAN ID	7	100	200	300	500
	VLAN Name	Mgmt_Vlan	Video_Vlan	Data_Vlan	Voice_Vlan	TLS_STAG Example
	Connection Type	Bridged	Bridged	Bridged	Bridged	TLS-Bridged
	Secure Forwarding	Disable	Disable	Disable	Disable	Enable
Port Membership	Fiber WAN (eth0)	T	T	T	T	-
	GE1 - GigE (eth1)	-	-	U	-	TLS
	GE2 - GigE (eth2)	-	-	U	-	-
	GE3 - GigE (eth3)	-	-	U	-	TLS
	GE4 - GigE (eth4)	-	-	U	-	-
	SSID 0 (wl0)	-	-	U	-	-
	SSID 1 (wl0_1)	-	-	-	-	-
	SSID 2 (wl0_2)	-	-	-	-	-
	SSID 3 (wl0_3)	-	-	-	-	-

Creating a TLS bridge

1 Set the VLAN Service Mode to S-Tag

Figure 162: Selecting S-Tag



Configuration - VLAN Modes

Transparent LAN Service Settings

VLAN Service Mode: S-Tag

S-Tag Ethernet Type: 8100

Global VLAN Routing Mode

Cross VLAN Routing: Disable

Global QOS Mode

Prioritization Method: Layer2 VLAN CoS

a Select **Configuration | VLAN | Modes**

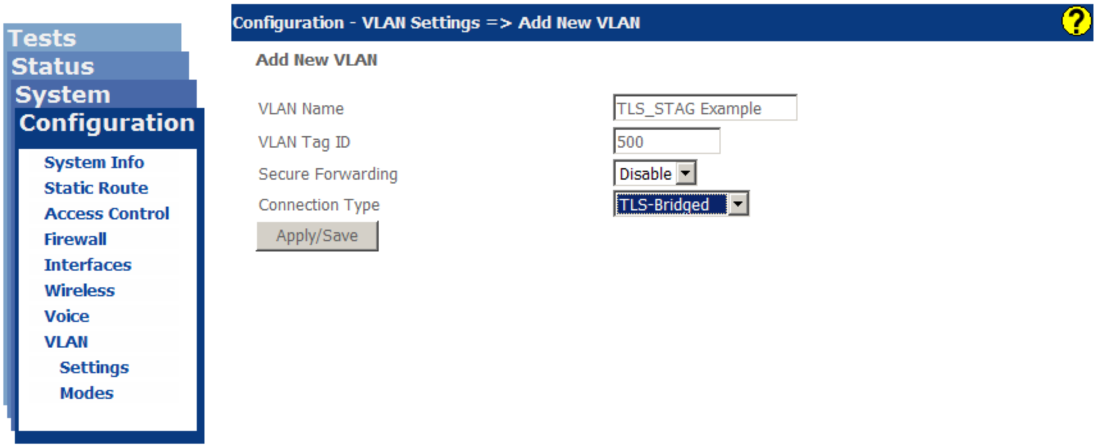
b On the **Configuration - VLAN Modes** page, select **S-Tag** from the **VLAN Service Modes** dropdown.

c Click **Apply**

2 Create a VLAN, select **TLS-Bridged**

If you have created other VLANs you will note that changing the mode adds an option to the connection type menu

Figure 163: Selecting TLS-Bridged



Configuration - VLAN Settings => Add New VLAN

Add New VLAN

VLAN Name: TLS_STAG Example

VLAN Tag ID: 500

Secure Forwarding: Disable

Connection Type: TLS-Bridged

a From the **Configuration | VLAN | Settings** page, click **Add New VLAN**

b In the **VLAN Name** text box enter a name for the VLAN

c In the **VLAN Tag ID** text box enter a VLAN ID

d <Optional> From the **Secure Forwarding** dropdown select either **Enable** or **Disable**

e From the **Connection Type** dropdown select **TLS-Bridged**

f Click **Apply/Save**

3 Select ports and set port defaults

a From the **Configuration - VLAN Settings => Edit Selected VLAN** page (which you should be on automatically after completing the previous step) Select the port members.

b From the **Port Membership** dropdown for the appropriate ports select **TLS**

Figure 164: Selecting port members and their tagging

For a single tagged TLS bridge interface we will select **TLS**. Selecting **S-TAG** would create an S-Tagged interface.

c Click **Save/Apply**

d From the **VLAN | Settings** page click **Edit Port Defaults**

Figure 165: Setting PVID for the ports

e In the **PVID** text box for **GE1 - GigE eth1**, enter 500 (the same as the ID for the VLAN)

f From the **Uplink** eth0 should be selected

Selecting the Fiber WAN interface adds this VLAN to the uplink.

g Click **Save/Apply**

NAT and DHCP

In this example the ONU will have all ports as untagged. The ONU will provide the IP addresses to the connected devices through DHCP. Note the each port has its own DHCP server. The addresses given out on each port must be in a different subnet. In this example, each port is set to give out 10 IP addresses. The ONU will perform NAT on the uplink interface to translate the public IP address to one of the private addresses.

With this configuration, the subscriber should be able to connect a PC to the Ethernet port, obtain an address and be ready to surf the Internet.

To setup NAT and DHCP

1 Define a routed VLAN

2 Define which ports are members of the VLAN

3 Set the PVID

Since this example is using untagged ports, it is critical to set the PVID to data VLAN. Otherwise all incoming packets will be dropped.

4 Enable NAT on the uplink port

Enable the NAT function, and set the DNS addresses. In this case we are using static addresses.

5 Enable DHCP and specify the range of addresses

Note the every port has its own DHCP server. Each port must be configured and must be on a separate subnet.

6 Verify the configuration

DHCP server

Dynamic Host Control Protocol (DHCP) is the means for dynamically assigning IP addresses. Basically, a DHCP server has a pool of IP addresses that can be assigned to DHCP clients. A DHCP client maintains its MAC address, but may have a different IP address each time it connects to the network. DHCP simplifies network administration since the DHCP server software tracks the used and unused IP addresses.

The zNID 24xx can act as a local DHCP server for devices connected on the LAN ports. In this mode, the zNID 24xx can assign temporary (leased) IP addresses to clients. Each DHCP client sends a request to the zNID 24xx for an IP address lease. The zNID 24xx then assigns an IP address and lease time to the client. The zNID 24xx keeps track of a range of assignable IP addresses from a subnetwork.

Some customers choose to have the same IP address every time their DHCP lease renews. This is known as sticky IP addresses. By default, the zNID 24xx attempts to assign the same IP address to the same client on DHCP lease renewal.

The DHCP server feature only works on routed interfaces. Typically, NAT would also be enabled to map the private addresses from the DHCP server to a public address.

Data services

Rate limiting

Rate limiting is done on a per-physical-port basis, not on a per-VLAN basis.

Rate limiting is a mechanism for controlling traffic and can include policing (dropping packets). Use rate limiting to control the rate of traffic sent or received on a physical port. Received traffic that is less than or equal to the specified rate is forwarded and traffic that exceeds the rate plus the max burst size is dropped.

After configuring an interface with rate limiting, the inbound traffic rate is monitored and if the rate exceeds the specified rate, a pause frame will be sent to the device connected to the port to stop the incoming traffic. If the connected device does not support pause frames, then the excessive data will be dropped.

The inbound and outbound rates are independent. This allows for symmetric or asymmetric rates (to emulate ADSL for example). The rate limiting in either direction can be disabled by entering 0 (zero) for the data rate.

For rate limits less than 100 Mbps, the rate can be set in 1Mbps increments. For rate limits greater than 100 Mbps, the rate must be set in 8 Mbps increments. The system will automatically adjust the value entered to an appropriate rate if necessary.

For the outbound direction, the data will be sent at the rate specified. Outbound data is mapped into different queues based on priority. Strict Priority scheduling is used for the Critical priority queue and WRR scheduling is used for the High, Medium and Low priority queues. The ratio is 16 packets from the high priority queue, 8 from the medium queue and 4 from the low priority queue.

The max Burst Size parameter specifies how much a single burst of data can exceed the inbound rate before packets are dropped. The default setting is 500k bytes.

Figure 166: Rate limits per interface

Priority

The system can be configured to prioritize traffic based on either the layer 2 VLAN CoS bits or the layer 3 ToS bits. The prioritization method is selected on the VLAN Mode page as shown below.

Figure 167: VLAN modes

The zNID 24xx products support the prioritization of traffic based on either the ToS (Type of Service) values in IP packets or CoS (Class of Service) values in Ethernet VLAN headers as defined by IETF RFC1349 and IEEE 802.1p respectively. The configured ToS or CoS levels specify packet priority and queuing used to transport the packet through the Ethernet and IP networks.

CoS

The VLAN header in Ethernet packets contains a CoS field for queuing priority or Class of Service (CoS) values based on eight (0-7) levels of service, with the lowest priority being 0 and the highest priority 7.

The eight priority values are mapped to 4 queues. The highest priority queue (Critical) uses strict priority. All the packets in that queue will be sent before any packets in the other queues. If there is a large amount of data in the strict priority queue, it is possible that the lower priority queues never get serviced. A weighted round robin approach is used for the remaining queues. The packets are sent in a ratio of 16 high priority, 8 Medium, and 4 Low priority.

Table 58: CoS value to priority mapping

CoS Value	Priority Queue	Priority Method
0	Low	WRR 16/8/4 (weight = 4)
1	Low	WRR 16/8/4 (weight = 4)
2	Med	WRR 16/8/4 (weight = 8)
3	Med	WRR 16/8/4 (weight = 8)
4	High	WRR 16/8/4 (weight = 16)

Table 58: CoS value to priority mapping

CoS Value	Priority Queue	Priority Method
5	High	WRR 16/8/4 (weight = 16)
6	Critical	Strict priority
7	Critical	Strict priority

Packets which require the highest throughput or are sensitive to latency (the amount of time between received packets) should be in higher priority queues. Normally video and voice are more sensitive to throughput and latency issues.

Precedence

IP packets have a ToS byte in their headers that contains information about relative priority. The IP Precedence field contains a 3-bit priority designation. Most normal traffic has an IP Precedence value of zero. Higher values in this field indicate that traffic is more important and that it requires special treatment. IP Precedence values greater than 5 are reserved for network functions.

The format of the ToS byte:

0	1	2	3	4	5	6	7
Precedence			D	T	R	Unused	

Table 59: Precedence values

Precedence Values	Priority Queue	Priority Method
0 (Routine)	Low	WRR 16/8/4 (weight = 4)
32 (Priority)	Low	WRR 16/8/4 (weight = 4)
64 (Immediate)	Med	WRR 16/8/4 (weight = 8)
96 (Flash)	Med	WRR 16/8/4 (weight = 8)
128 (Flash Override)	Med	WRR 16/8/4 (weight = 16)
160 (Critical)	High	WRR 16/8/4 (weight = 16)
192 (Internetwork Control)	Critical	Strict priority
224 (Network Control)	Critical	Strict priority

Note: Data is prioritized using only the Precedence bits, not the entire Diffserv field.

4 SPECIAL SCENARIOS

This chapter describes troubleshooting tests for the zNID 24xx. It includes the following sections:

Zhone supports the Microsoft Media Room (MMR) application in many deployments for GPON, ADSL and VDSL. Zhone’s IPTV deployment includes support for integrated residential gateway functionality required by MMR to significantly reduce the complexity and cost of deployments.

With any port, any service there is no need to designate some Ethernet Ports as “data” ports and others as “video” ports. IPTV streams can be watched from PCs using media streaming applications, or VoD and Pay per view content may be viewed. Set top boxes (STBs) can join IPTV streams, access VoD content or browse the Internet. Game consoles can access online gaming over the Internet, browse the Internet, watch IPTV streams or access VoD content.

This chapter includes the following sections

Microsoft Media Room support

MMR provides live, recorded, and on demand programming for PCs, mobile phones and TV. All MMR client devices in the home must be able to discover each other and communicate freely with each other. For this reason, all client devices must be locally bridged with IP Addresses in the same subnet. For security reasons, client devices in one customer’s home must not be able to discover MMR client devices in other customers’ homes. As a result, NAT Routing is required to provide firewall security.

Figure 168: MMR provides live, recorded, and on demand programming for PCs, media servers (like the Xbox) and TV

The wire speed NAT Routing capabilities of Zhone’s zNID product family are required to support multiple concurrent High Definition IP TV streams with low latency and no packet loss. This is just one of the key attributes of the zNID product line required to support the integrated MMR Home Gateway capability.

There are several Residential Gateway requirements introduced by the MMR application, and Zhone’s zNID 24xx supports them all.

The Zhone MMR application described in this document shows the high level configuration items and describes how the zNID 24xx ONT provides data and IPTV services to downstream set top boxes and media servers.

The MXK aggregates the services for Internet, IP video, and Video on Demand (VoD) segregating the services by VLAN. The zNID uses the VLAN segregation to provide video services to IPTV, Media server and PCs.

Figure 169: The zNID 24xx includes integrated support for the MicroSoft Media Room 2.0 Application

zNID Configuration requirements for MMR:

- Two NAT BRouted VLANs must be created. All zNID LAN ports must be UNTAGGED members of both VLANs. The zNID Uplink must be TAGGED member of both. DHCP Server is enabled on the Data VLAN. UPnP enabled on DATA VLAN.
- IGMP Snooping must be enabled on the Video VLAN.
- All local Ethernet traffic untagged, with Default PVID = Data VLAN, IGMP PVID = Video VLAN.
- All local devices have private IP addresses in the same subnet (assigned by zNID DHCP server) and communicate freely with each other.
- Conditional DHCP Addressing is used to assign permanent IP Address to STBs and DVRs based on OUI classification. These devices are assigned IP addresses from a dedicated range within the subnet.
- All Data VLAN traffic is locally Bridged.
- All LAN broadcast traffic is kept LOCAL.
- Cross VLAN Routing must be enabled (for VoD traffic).
- All upstream traffic on the Data VLAN is NAT Routed out the vlan500 vs. vlan600 WAN uplink based on Route Table lookup (based on Dest IP). If there isn't a match in the Route Table, the Default Route will be to use the Data VLAN.
- Static Routes must be created for the IP Address ranges used for unicast Video Traffic (e.g. VoD). DHCP Option 121 can create these automatically.
- Downstream unicast traffic from vlan500 and vlan600 is NAT Routed to the vlan500 LAN side client device.
- Downstream multicast video traffic on vlan600 is Bridged only to the port(s) that JOINED the stream.
- DNS Proxy must be enabled. Static DNS Entries must be configured for discovery.iptv.microsoft.com, resolving to the IP Address of the Service Provider's MMR Head End.
- Static DNS Entries must be configured for any other Domain Names that won't resolve using the Public DNS.

Any port, any service

Zhone supports the concept that any device connected to the zNID 24xx can access any service, whether that service is high speed Internet (HSIA), IPTV or Video on Demand (VoD) from any Ethernet port. With up to four Gigabit Ethernet ports as well as two POTS port there is enough bandwidth to supply HSIA, IPTV and VoD as well as analog telephone.

With any port, any service there is no need to designate some Ethernet Ports as “data” ports and others as “video” ports. IPTV streams can be watched from PCs using media streaming applications, or VoD and Pay per view content may be viewed. Set top boxes (STBs) can join IPTV streams, access VoD content or browse the Internet. Game consoles can access online gaming over the Internet, browse the Internet, watch IPTV streams or access VoD content.

Figure 170: Zhone zNID products include integrated support any port and service on the GE LAN ports

zNID configuration requirements for any port, any service:

- Each service must have a unique VLAN.
- IGMP Snooping must be enabled on the Video VLAN.
- All local Ethernet traffic untagged, with Default PVID = Data VLAN, IGMP PVID = Video VLAN.
- All local devices have private IP addresses in the same subnet (assigned by zNID DHCP server) and communicate freely with each other.

- Conditional DHCP Addressing is used to assign permanent IP Address to STBs and DVRs based on OUI classification. These devices are assigned IP addresses from a dedicated range within the subnet.
- All LAN broadcast traffic is kept LOCAL
- Cross VLAN Routing must be enabled (for VoD traffic)
- Static Routes must be created for the IP Address ranges used for unicast Video Traffic (e.g. VoD). DHCP Option 121 can create these automatically.
- Analog phones or fax machines are supported on the POTS interfaces.
- Note that the WiFi interfaces do not support IPTV

5 TROUBLESHOOTING TESTS

This chapter describes troubleshooting tests for the zNID 24xx. It includes the following sections:

- Diagnostics, page 219
- Ping, page 221
- Trace route, page 222
- Hardware reset, page 224

Diagnostics

The Diagnostics page runs tests on each interface. If a test shows **FAIL**, click the **Hints** link to diagnose the issue.

Figure 171: The Diagnostics page

The Ethernet connection test checks whether the zNID detects a device connected, so the hints will be cabling and whether the device is running properly. Restarting most devices will put them in a known state.

Figure 172: Example of the hints for failing an Ethernet connection test.

Ping

The Ping test sends an IP ping to an IP address. The ping can be used to determine if another device can be accessed from the zNID.

Figure 173: The Ping test

Table 60: Ping test parameters

Parameter	Description
IP Address or Domain Name	The destination address can be entered as a dot notation IP address (i.e. 135.20.3.40) or a Domain Name to be looked up on the configured Domain Name Server.
Length of packet	The number of bytes in the IP Payload portion of the packet. Additional bytes for packet overhead are normally added as well so the length of the overall packet is longer. Setting the value larger than 64 can determine problems in a network that restrict large packets. The default is 64. Setting the value larger than 64 can determine problems in a network that restrict large packets. The default is 64.
Count	The number of pings to be sent before the test completes. A large number will allow the user to verify network connectivity during certain testing. The default is 4.

Trace route

The Trace Route test issues an ICMP echo command to the destination address. The result shows the path (hops) it took to reach the destination address.

Figure 174: The Trace Route test

Table 61: Trace route parameter

Parameter	Description
IP Address or Domain Name	The final destination can be entered as a dot notation IP address (i.e. 135.20.3.40) or a Domain Name to be looked up on the configured Domain Name Server.
Max Time to Live	**Max Time to Live** is the maximum number of “hops” or nodes that the packet is allowed to traverse before quitting the test. The default is 30.
Queries Per Hop	The number of times the test will go to each hop count. The **Queries Per Hop** number must be greater than 1. The default is 3.
Wait Per Response	The number of seconds to wait for the echo response. The default is 3.

Voice

Figure 175:

Hardware reset

To reset the zNID 24xx

1. Press a pin into the reset button and hold it down until all LEDs are on together.
2. Release the reset button.

INDEX