VITESSE®

Layer 2 Protocol Configuration Guide

Application Note

VPPD-03596 / AN1115
Revision 1.3
Nov 2014

Vitesse

www.vitesse.com

TERMS OF USE

The information provided by Vitesse Semiconductor Corporation ("Vitesse") in this document pursuant to these terms ("Agreement") is intended for illustrative purposes only. All information provided herein is subject to change at any time without notice. The information provided, including but not limited to Sample Code ("Software"), is protected by United States and other applicable copyright laws and international treaties. Vitesse does not grant You any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

ALL INFORMATION, INCLUDING BUT NOT LIMITED TO THE SAMPLE CODE ("CODE ") SUPPLIED, IS PROVIDED STRICTLY "AS-IS" WITH NO WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, MADE WITH RESPECT TO THE INFORMATION TO INCLUDE THE CODE AND ALL ACCOMPANYING WRITTEN MATERIALS, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. YOU ASSUME THE ENTIRE RISK AS TO THE QUALITY, ACCURACY, AND PERFORMANCE OF THE INFORMATION, AND YOU ASSUME ANY AND ALL RISK AND LIABILITY FOR ANY ACTIONS TAKEN BY YOU ON THE BASIS OF ITS ANALYSIS OR OTHER USE OF THE INFORMATION, INCLUDING BUT NOT LIMITED TO MODIFICATIONS TO YOUR PRODUCTS IN LIGHT OF SUCH USE OF INFORMATION, AND YOU HEREBY ACKNOWLEDGE THAT VITESSE SHALL HAVE NO RESPONSIBILITY OR LIABILITY AS A RESULT OF YOUR USE OF INFORMATION PROVIDED HEREUNDER.

IN NO EVENT SHALL VITESSE BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF USE OR INABILITY TO USE THE CODE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This Agreement is governed by the laws of the State of California, without regard to principles of conflicts of laws. Each provision of this Agreement is severable. If a provision is found to be unenforceable, this finding does not affect the enforceability of the remaining provisions of this Agreement. This Agreement is binding on successors and assigns. By accessing the information contained in or referenced by this document, You acknowledge that You have read this Agreement, that You understand it, that You agree to be bound by its terms, and that this is the complete and exclusive statement of the Agreement between You and Vitesse regarding the information and Code.

Contents

Figures

Revision History

Revision	Date	Description
Rev 1.0	December 18, 2013	First release
Rev 1.1	March 14, 2014	Added CEService case to GVRP section
Rev 1.2	July 28, 2014	Updated template
Rev 1.3	November, 2014	Editorial updates

1 Introduction

This document describes how to configure Vitesse Switch Engine devices to perform Layer 2 functions such as Link Aggregation (LAG), Link Aggregation Control Protocol (LACP), Virtual LANs (VLANs), Mirroring, Generic VLAN Registration Protocol (GVRP), and Multiple Spanning Tree Protocol (MSTP). Configuration examples are provided both for the command line interface (CLI) and the Web GUI.

2 Aggregation

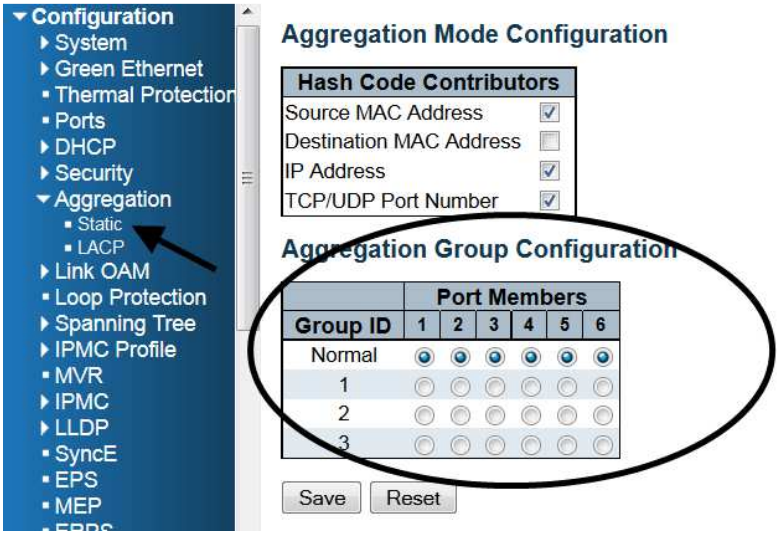
Aggregation enables the use of multiple ports in parallel to increase the link speed beyond the limits of a single port and to increase the redundancy for higher availability. If the system has 6 ports, the maximum aggregation group is 3 (6 divided by 2).

2.1 Adding a Port to an Aggregation Group

CLI Example: Add the first Gigabit port into group 1

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# aggregation ?
    group    Create an aggregation group
(config-if)# aggregation group
<uint>
(config-if)# aggregation group 1
```

Figure 1. Web GUI: Aggregation Group Configuration



2.2 Configuring the Aggregation Mode

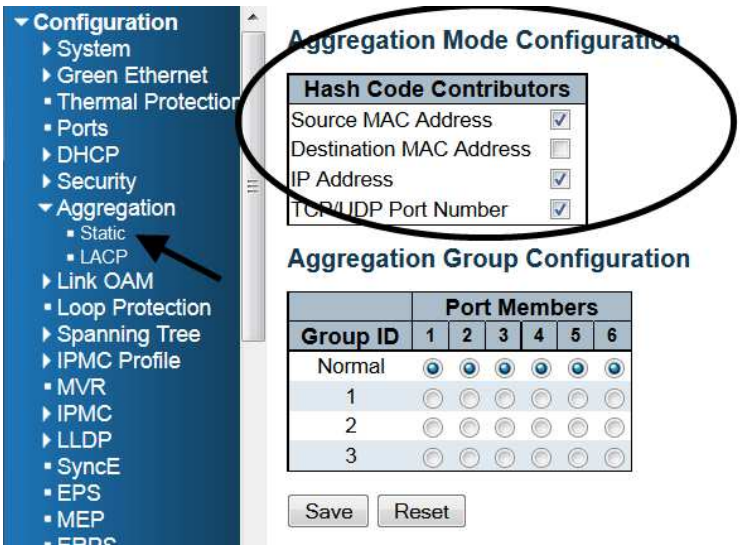
The aggregation feature can use the following keys to calculate the destination port for the frame. The default method is the Source MAC Address, IP Address and TCP/UDP Port Number. The Destination MAC Address is not used in the default case.

CLI Example: Change aggregation mode to dmac, ip, port and smac

```
# configure terminal
(config)# aggregation mode ?
    dmac    Destination MAC affects the distribution
    ip      IP address affects the distribution
    port    IP port affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggregation mode dmac ip port smac
(config)# do show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Enabled
IP    : Enabled
Port  : Enabled
```

Figure 2. Web GUI: Aggregation Mode Configuration



The current aggregation mode can be viewed with the **show aggregation mode** command as seen here:

```
# show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
```

3 LACP

Link Aggregation Control Protocol (LACP) is an IEEE 802.3ad standard protocol that allows bundling several physical ports together to form a single logical port.

3.1 Enabling LACP

When LACP is enabled on a port, with the **lacp** command, it will form an aggregation when 2 or more ports are connected to the same partner. The default value is disabled.

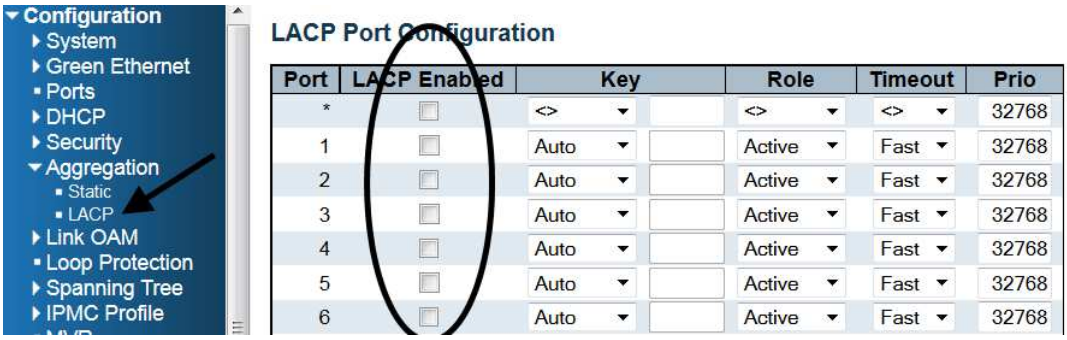
CLI Example: Enable LACP on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
```

CLI Example: Disable LACP on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# no lacp
```

Figure 3. Web GUI: LACP Enabled Configuration



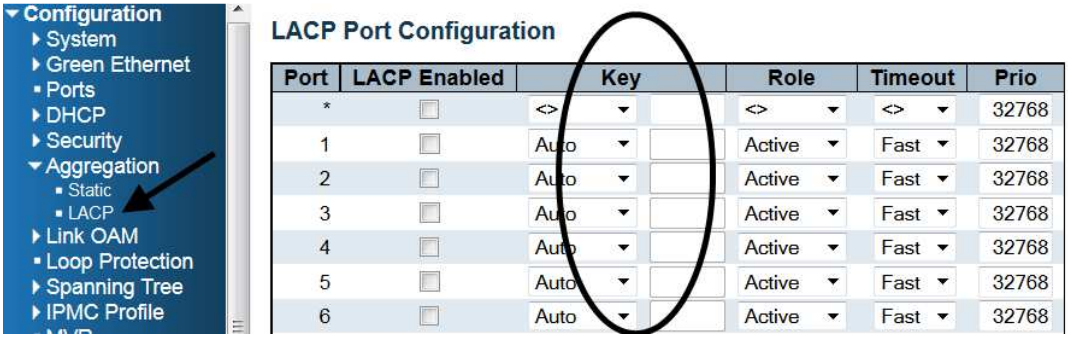
3.2 Configuring the Key

The port's LACP Key ranges from 1-65535. The Auto setting will set the key according to the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. With a specific setting a user-defined value can be entered. Ports with the same Key can participate in the same aggregation group while ports with different keys cannot. The default value is auto.

CLI Example: Set LACP key to 3 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp key ?
    <1-65535>    Key value
    auto         Choose a key based on port speed
(config-if)# lacp key 3
```

Figure 4. Web GUI: LACP Key Configuration



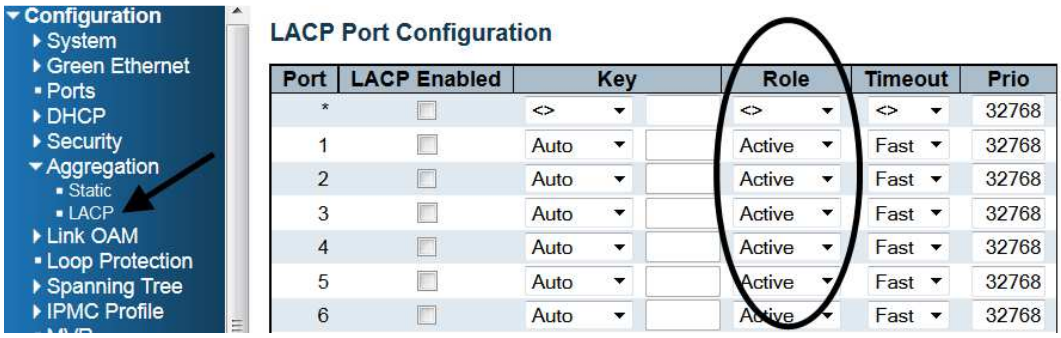
3.3 Configuring the Role

LACP Role shows the activity status. An Active Role will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner, also known as the "speak if spoken to" role. The default value is active.

CLI Example: Set LACP Role to Passive on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp role ?
    active     Transmit LACP BPDUs continously
    passive    Wait for neighbour LACP BPDUs before transmitting
(config-if)# lacp role passive
```

Figure 5. Web GUI: LACP Role Configuration



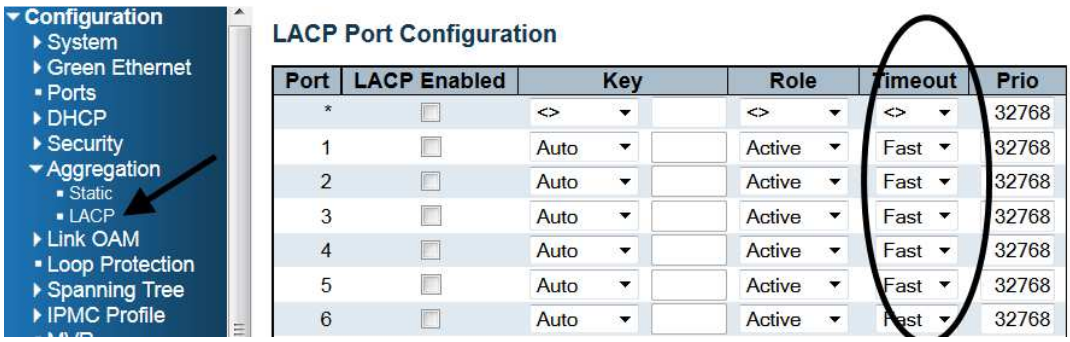
3.4 Configuring the Timeout

The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second while Slow will wait for 30 seconds before sending a LACP packet. The default value is fast.

CLI Example: Set LACP Timeout to slow on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp timeout ?
    fast    Transmit BPDU each second (fast timeout)
    slow    Transmit BPDU each 30th second (slow timeout)
(config-if)# lacp timeout slow
```

Figure 6. Web GUI: LACP Timeout Configuration



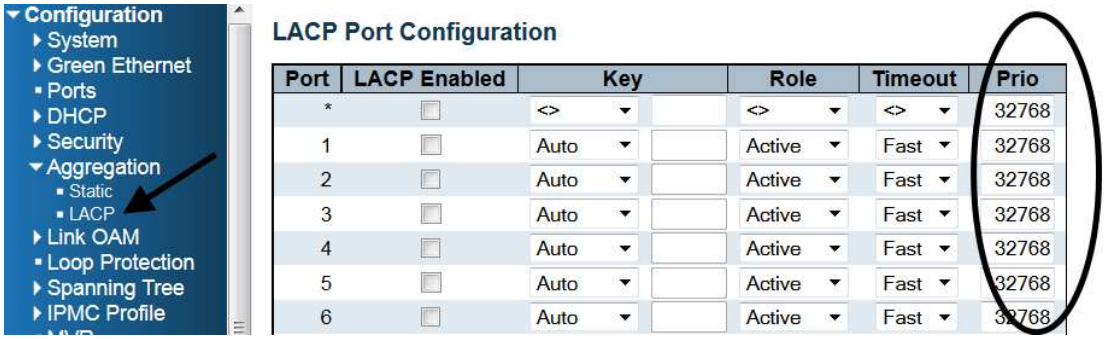
3.5 Configuring the Priority

The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active and which ports will be in a backup role. Lower numbers mean greater priority. The default value is 32768.

CLI Example: Set LACP priority to 1000 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp port-priority ?
    <1-65535>    Priority value, lower means higher priority
(config-if)# lacp port-priority 1000
```

Figure 7. Web GUI: LACP Prio Configuration



3.6 Showing the Status

The current LACP mode can be viewed with the **show lacp** command as seen here**:**

```
# show lacp ?
    internal      Internal LACP configuration
    neighbour     Neighbour LACP status
    statistics    Internal LACP statistics
    system-id     LACP system id
```

4 MAC Address Table

Switching is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to. This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a source MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

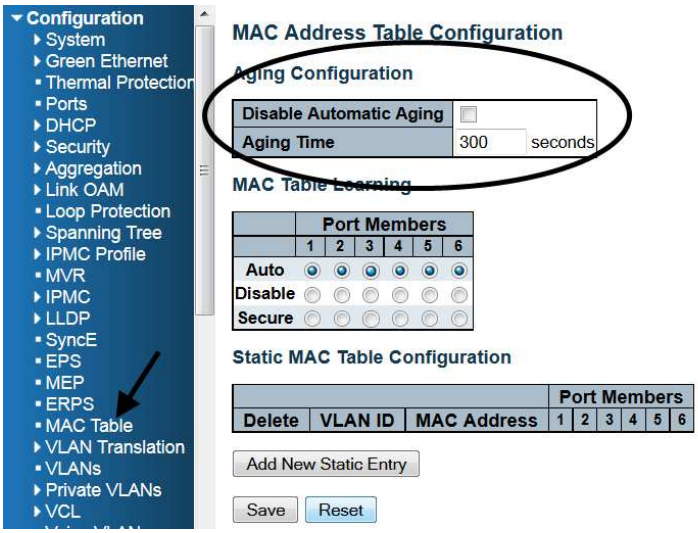
4.1 Setting the Aging Time

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.

CLI Example: Change the aging time to 600 seconds

```
# configure terminal
(config)#
(config)# mac address-table aging-time ?
    <0,10-1000000>    Aging time in seconds, 0 disables aging
(config)# mac address-table aging-time 600
```

Figure 8. Web GUI: MAC Address Table Aging Configuration

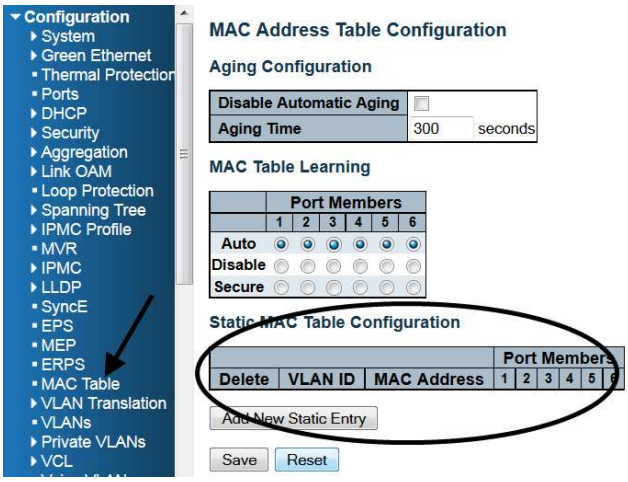


4.2 Adding a Static MAC Address Entry

CLI Example: Add the static MAC address: 00:00:00:00:00:01 in VLAN 2 on the first Gigabit port

```
# configure terminal
(config)#
(config)# mac address-table ?
    aging-time    Mac address aging time
    static        Static MAC address
(config)# mac address-table static 00:00:00:00:00:01 vlan 2 interface
GigabitEthernet 1/1
```

Figure 9. Web GUI: Static MAC Address Configuration

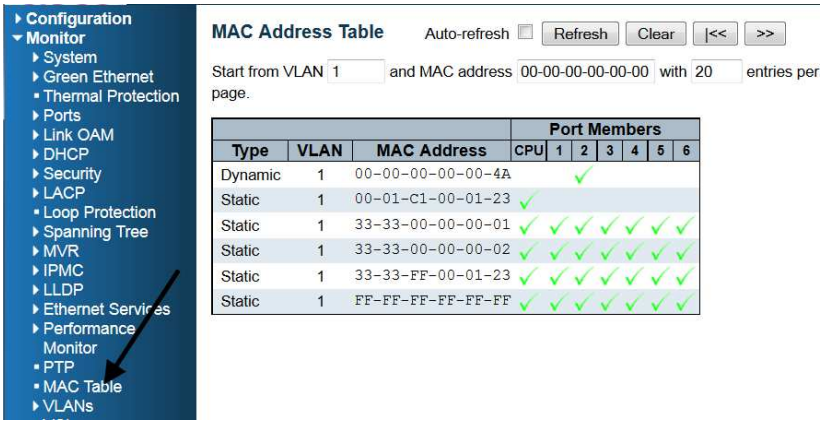


4.3 Showing the MAC Address Table

The current MAC address table can be viewed with the **show mac address-table** command as seen here**:**

```
# show mac address-table
```

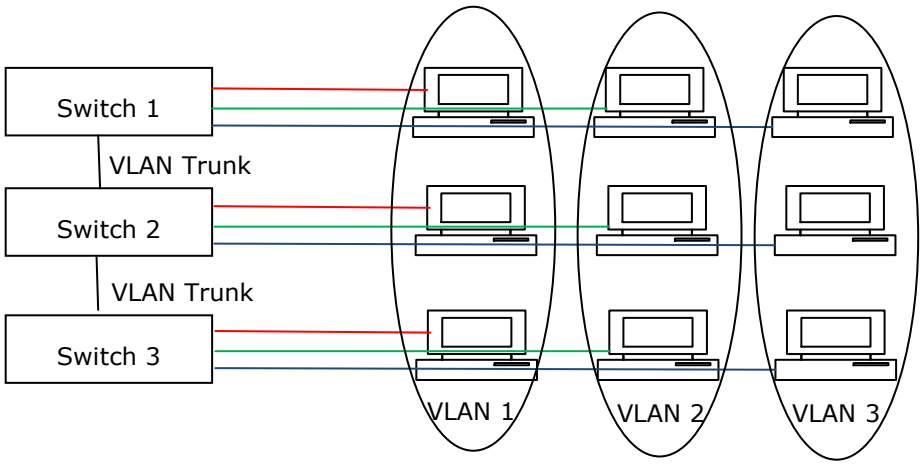
Figure 10. Web GUI: MAC Address Table



5 VLAN

5.1 Quick Start

Figure 11. VLAN Quick Configuration Example



Since VLAN 1 is created by default, one must only add VLAN 2 and 3 as follows:

```
# configure terminal
(config)# vlan 2
(config)# vlan 3
```

Set the Access port as shown below. In this case it is assumed that port 1 through3 are connected to the PC. The PVID of each port is different.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 1
(config)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config)# exit
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config)# exit
```

Set the Trunk port. It is assumed that port 4 is connected to the other switch. Set the allowed vlan to accept 1-3.

```
# configure terminal
(config)# interface GigabitEthernet 1/4
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-3
```

Configure the port such that frames are always transmitted with a tag on port 4.

```
(config-if)# switchport trunk vlan tag native
```

5.2 Global Configuration

5.2.1 Existing VLAN

CLI Example: Adding VLAN 2

```
# configure terminal
(config)# vlan 2
```

CLI Example: Removing VLAN 2

```
# configure terminal
(config)# no vlan 2
```

CLI Example: Show existing VLANs

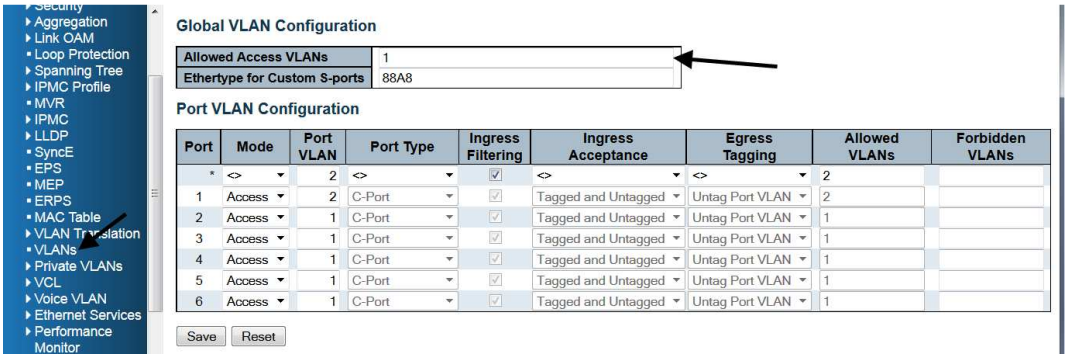
```
# show vlan brief
VLAN  Name                                Interfaces
----  --------------------------------    ----------
1     default                             Gi 1/1-6
2     VLAN0002
```

This Allowed Access VLAN field only affects ports configured as Access ports, discussed further in section 5.3.1. Ports in other modes are members of all VLANs specified in the allowed VLANs field, described in section 5.3.7. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax as shown below:

```
# configure terminal
(config)# vlan 1,10-13,200,300
```

Individual elements are separated by commas and ranges are specified with a dash separating the lower and upper bound. Spaces are allowed in between the delimiters. The above example will create VLANs 1, 10, 11, 12, 13, 200, and 300.

Figure 12. Web GUI: VLAN Allowed Access VLANs Configuration



5.2.2 VLAN Naming

CLI Example: Set VLAN2's name to test

```
# configure terminal
(config)# vlan 2
(config-vlan)# name test
```

Web GUI

Not available.

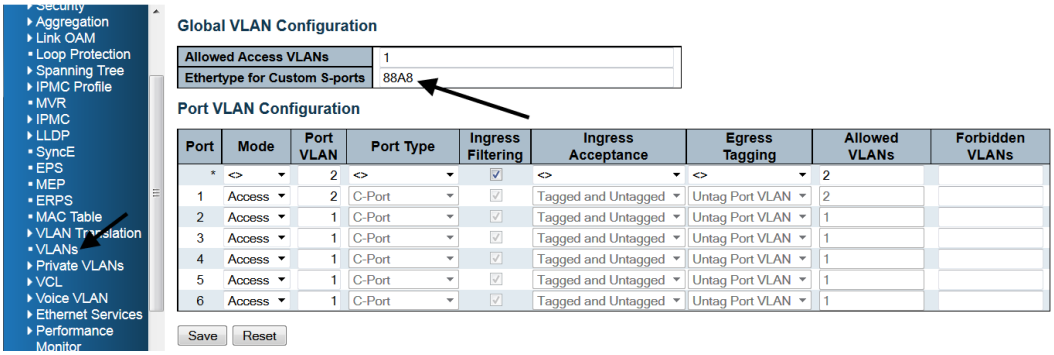
5.2.3 Ethertype for Custom S-ports

This field specifies the Ethertype/TPID (specified in hexadecimal) of tagged frames. The setting applies to all ports whose Port Type is set to S-Custom-Port. It takes effect on the egress side.

CLI Example

```
# configure terminal
(config)# vlan ethertype s-custom-port
<0x0600-0xffff>
```

Figure 13. Web GUI: VLAN Ethertype for Custom S-ports Configuration



5.3 Port Based Configuration

5.3.1 Port Mode

The port mode determines the fundamental behavior of the port in question. A port can be in one of three modes as described below with Access being the default.

Access:

Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- member of exactly one VLAN, the Port LAN or Access VLAN, which by default is 1,
- accepts untagged frames and C-tagged frames,
- discards all frames that are not classified to the Access VLAN, and
- upon egress all frames are transmitted untagged.

Trunk:

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- by default, a trunk port is member of all existing VLANs (see section 5.2.1). This may be limited by the use of Allowed VLANs (see section 5.3.7),

- by default, all frames but frames classified to the Port VLAN or Native VLAN get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
- egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid:

Hybrid ports resemble trunk ports in many ways while including additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
- ingress filtering can be controlled,
- ingress acceptance of frames and configuration of egress tagging can be configured independently.

CLI Example: Configure as Access port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
```

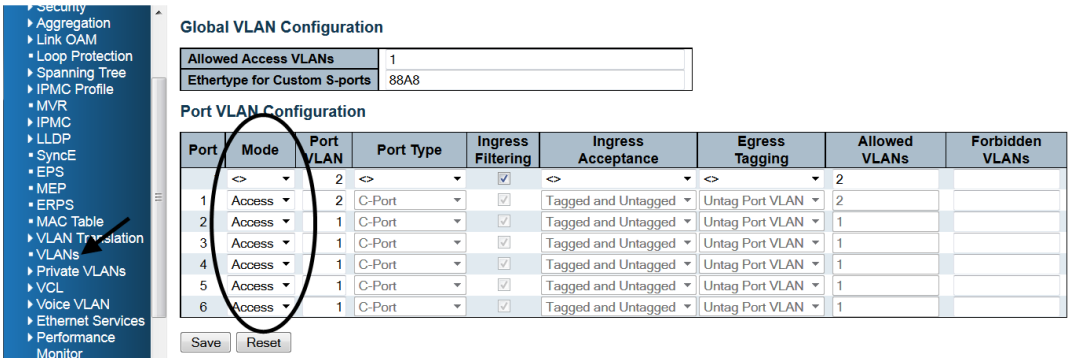
CLI Example: Configure as Trunk port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode trunk
```

CLI Example: Configure as Hybrid port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
```

Figure 14. Web GUI: VLAN Mode Configuration



5.3.2 Port VLAN

The Port VLAN determines the port's VLAN ID, or PVID. Allowed VLANs are in the range of 1 through 4095, with the default being 1.

Upon ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging (see section 5.3.6) is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and "Native VLAN" for ports in Trunk or Hybrid mode.

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as access mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 2
    <vlan_id>    VLAN ID of the native VLAN when this port is in trunk mode
```

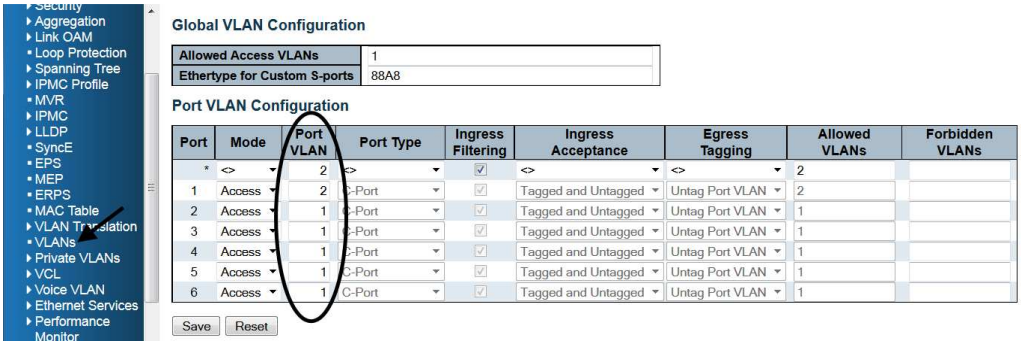
CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as trunk mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk native vlan 2
```

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 2
```

Figure 15. Web GUI: VLAN PVID Configuration



5.3.3 Port Type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware:

On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port:

On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port:

On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

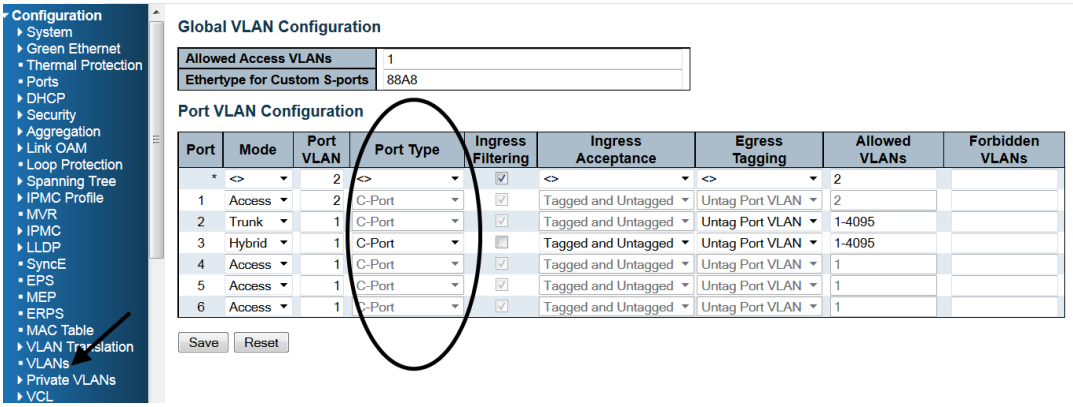
S-Custom-Port:

On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports (see section 5.2.3) get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

CLI Example: Set Port Type on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid port-type ?
    c-port           Customer port
    s-custom-port    Custom Provider port
    s-port           Provider port
    unaware          Port in not aware of VLAN tags.
```

Figure 16. Web GUI: VLAN Port Type Configuration



5.3.4 Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

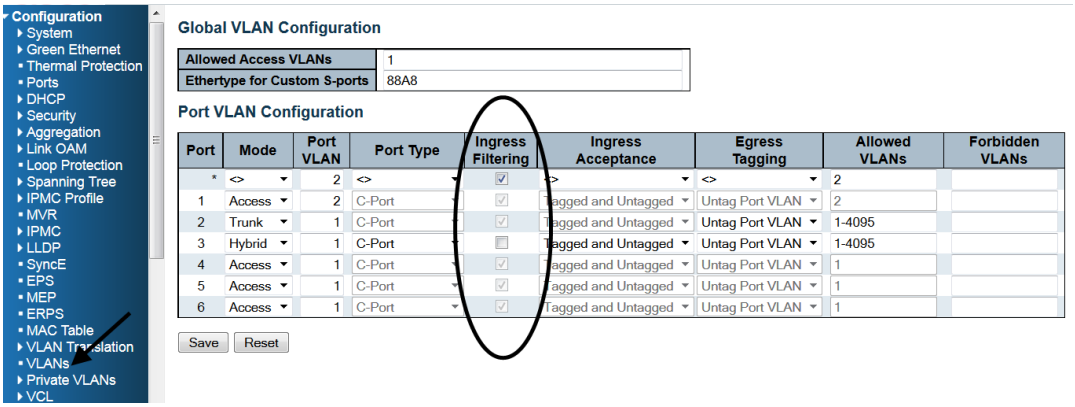
If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

CLI Example: Set ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid ?
    acceptable-frame-type    Set acceptable frame type on a port
    allowed                  Set allowed VLAN characteristics when interface is
                             in hybrid mode
    egress-tag               Egress VLAN tagging configuration
    ingress-filtering        VLAN Ingress filter configuration
    native                   Set native VLAN
```

```
    port-type                Set port type
```

Figure 17. Web GUI: VLAN Ingress Filtering Configuration



5.3.5 Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged

Both tagged and untagged frames are accepted.

Tagged Only

Only tagged frames are accepted on ingress. Untagged frames are discarded.

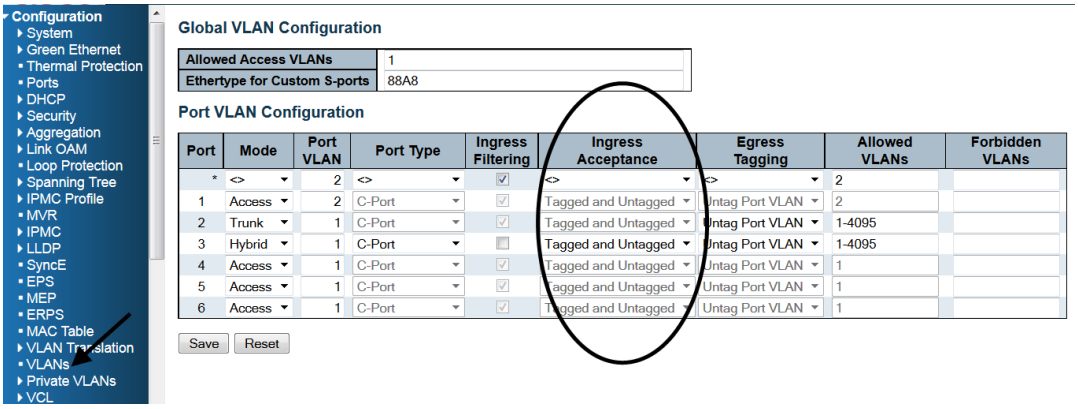
Untagged Only

Only untagged frames are accepted on ingress. Tagged frames are discarded.

CLI Example: Configure ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid acceptable-frame-type ?
    all          Allow all frames
    tagged       Allow only tagged frames
    untagged     Allow only untagged frames
```

Figure 18. Web GUI: VLAN Ingress Acceptance Configuration



5.3.6 Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN

Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

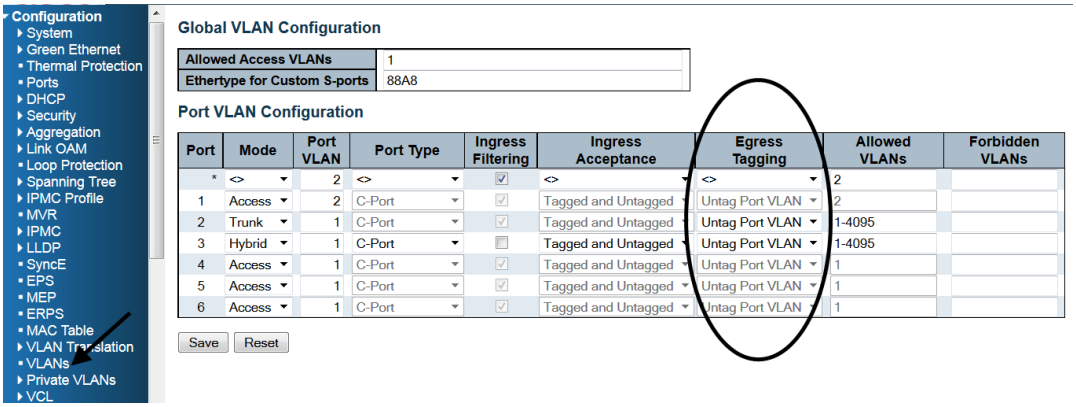
Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

CLI Example: Set egress tagging on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid egress-tag ?
    all     Tag all frames
    none    No egress tagging
```

Figure 19. Web GUI: VLAN Egress Tagging Configuration



5.3.7 Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the Existing VLANs field (see section 5.2.1). By default, a port may become a member of all possible VLANs, and is therefore set to `1-4095`.

The field may be left empty, which means that the port will not be member of any of the existing VLANs.

CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as trunk mode)

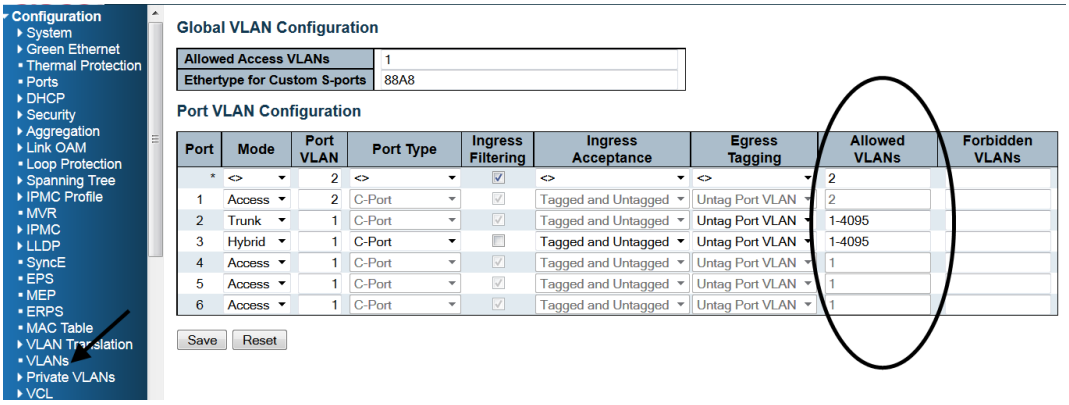
```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk allowed vlan ?
```

```
    <vlan_list>    VLAN IDs of the allowed VLANs when this port is in hybrid
                   mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
```

CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid allowed vlan ?
    <vlan_list>    VLAN IDs of the allowed VLANs when this port is in hybrid
                   mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
```

Figure 20. Web GUI: Allowed VLANs Configuration



5.3.8 Forbidden VLANs

A port may be configured to never be a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

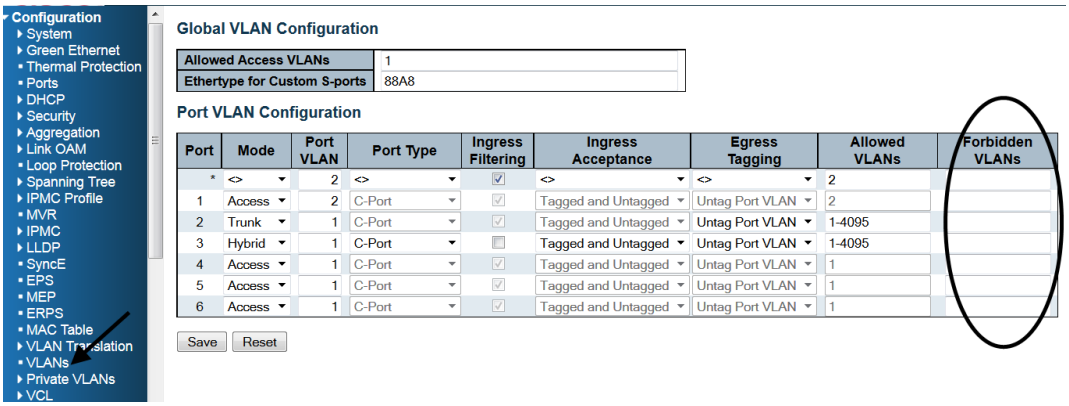
The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field (see section 5.2.1).

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

CLI Example: Configure forbidden VLAN on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport forbidden vlan ?
    add       Add to existing list.
    remove    Remove from existing list.
```

Figure 21. Web GUI: Forbidden VLANs Configuration



5.3.9 Show VLAN Status

CLI Example

```
# show vlan ?
    brief         VLAN summary information
    id            VLAN status by VLAN id
    ip-subnet     Show VLAN ip-subnet entries.
    mac           Show VLAN MAC entries.
    name          VLAN status by VLAN name
    protocol      Protocol-based VLAN status
    status        Show the VLANs configured for each interface.
    <cr>
```

Web GUI

Various internal software modules may use VLAN services to configure VLAN memberships on the fly, like NAS, GVRP, MVR, Voice VLAN, MEP, or EVC.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software module configuration, and basically reflect what is actually configured in hardware.

Figure 22. Web GUI: VLAN Membership Status

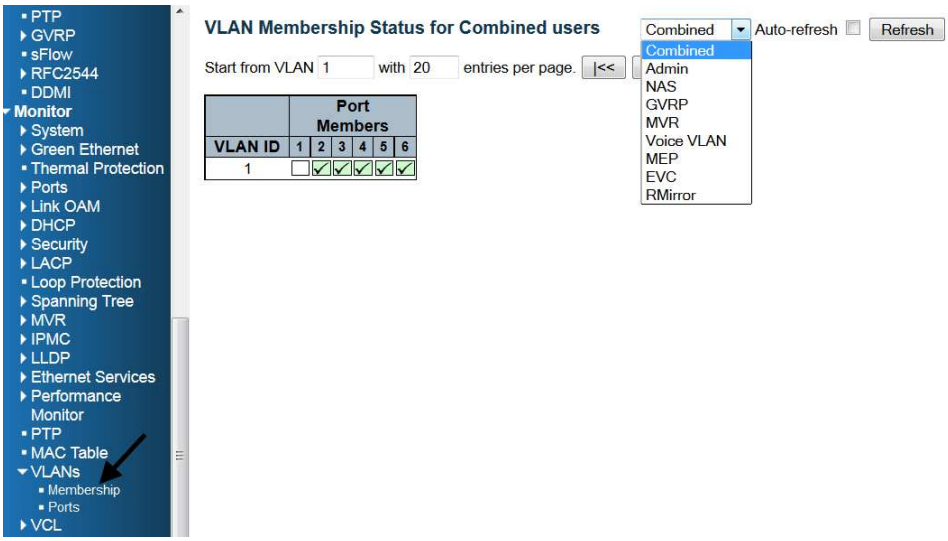
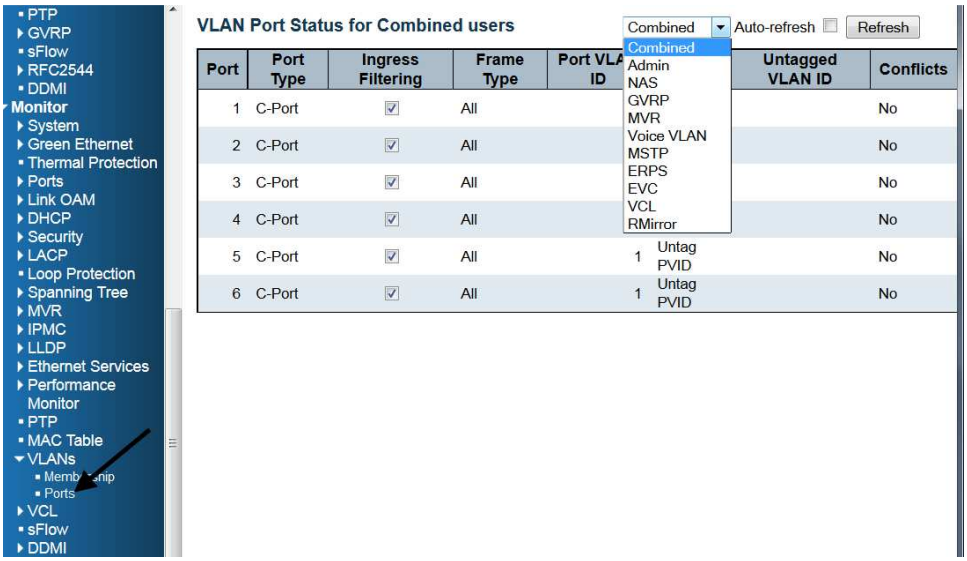


Figure 23. Web GUI: VLAN Port Status



6 Mirroring and Remote Mirroring

6.1 Mirroring (Local)

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port.

6.1.1 Mirror the Traffic of Port X to Port Y

Enable Mirror session

```
# configure terminal
```

```
(config)# monitor session 1
```

Mirror the traffic (both rx and tx) of the first Gigabit port

```
(config)# monitor session 1 source interface GigabitEthernet 1/1 both
```

Configure the mirror destination port to Gigabit port 6

```
(config)# monitor session 1 destination interface GigabitEthernet 1/6
```

Verify the monitor setting

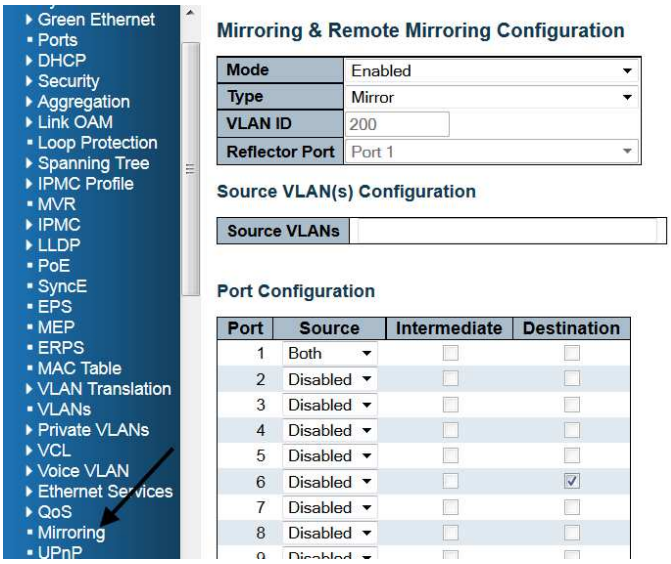
```
(config)# end
# show monitor session 1

Session 1
---------
Mode                     : Enabled
Type                     : Mirror
Source VLAN(s)           :
Source Ports             :
    Both                 : 1/1
Destination Ports        : 1/6
```

Disable Mirror session

```
# configure terminal
(config)# no monitor session 1
```

Figure 24. Web GUI: Mirror Traffic of Port 1 to Port 6



6.1.2 Mirror the Traffic of VLAN N to Port Y

Enable Mirror session

```
# configure terminal
(config)# monitor session 1
```

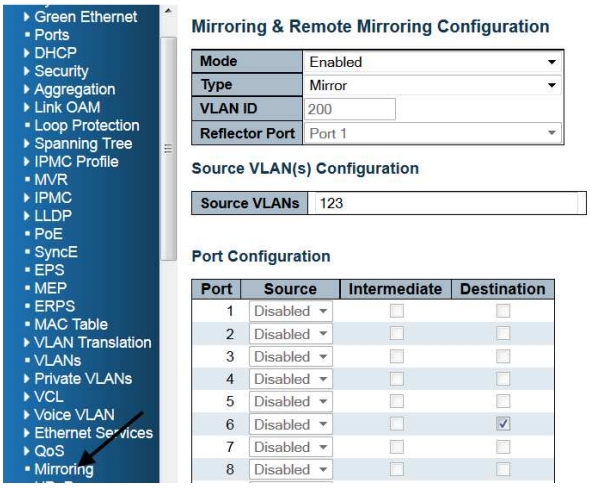
Mirror the traffic of VLAN 123

```
(config)# monitor session 1 source vlan 123
```

Configure the mirror destination port to Gigabit port 6

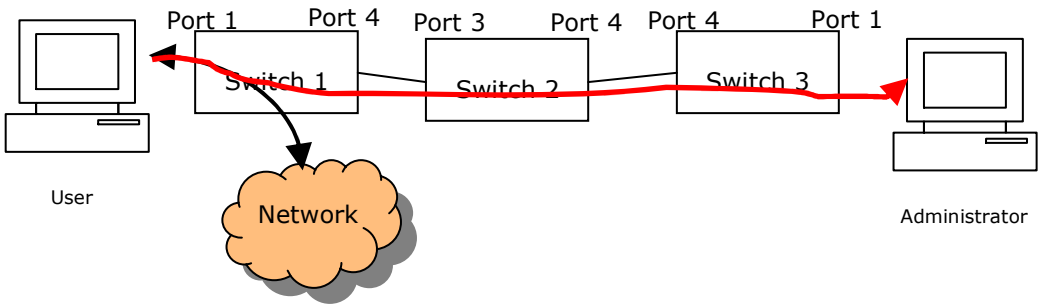
```
(config)# monitor session 1 destination interface GigabitEthernet 1/6
```

Figure 25. Web GUI: Mirror Traffic of VLAN 123 to Port 6



6.2 Remote Mirroring

Remote Mirroring is an extended function of Mirroring. It can extend the destination port in other switches. So the administrator can analyze the network traffic on the other switches.



Switch 1

Configure Switch 1 as the Source Switch with the following parameters

- Source port: 1
- Mirror mode: both, frames received and frames transmitted are mirrored.
- Intermediate port: 4

  Note The intermediate port needs to disable MAC Table learning.
- Reflector port: 2

  Note1 The reflector port needs to select only on Source switch type.

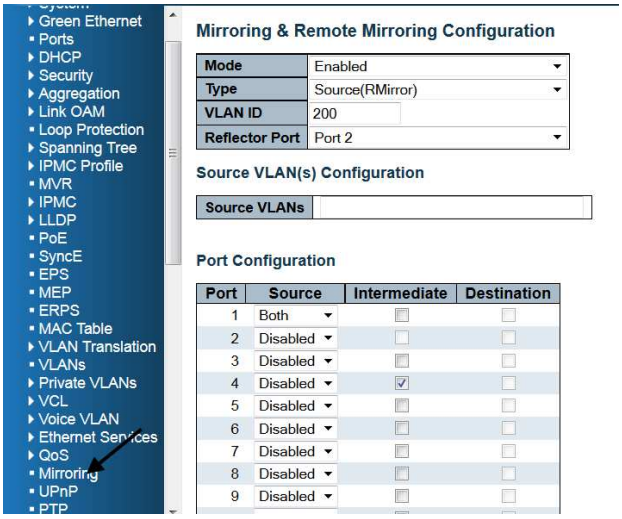
  Note2 The reflector port needs to disable MAC Table learning and STP.

  Note3 The reflector port is only supported on pure copper ports.
- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - source switch configuration

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 source interface GigabitEthernet 1/1 both
(config)# monitor session 1 intermediate interface GigabitEthernet 1/4
(config)# monitor session 1 destination remote vlan 200 reflector-port
GigabitEthernet 1/2
(config)# interface GigabitEthernet 1/2
(config-if)# no spanning-tree
(config-if)# no mac address-table learning
```

Figure 26. Web GUI: Remote Mirroring - Source Switch



Switch 2

Configure Switch 2 as Intermediate Switch with the following parameters

- Intermediate port: 3 and 4

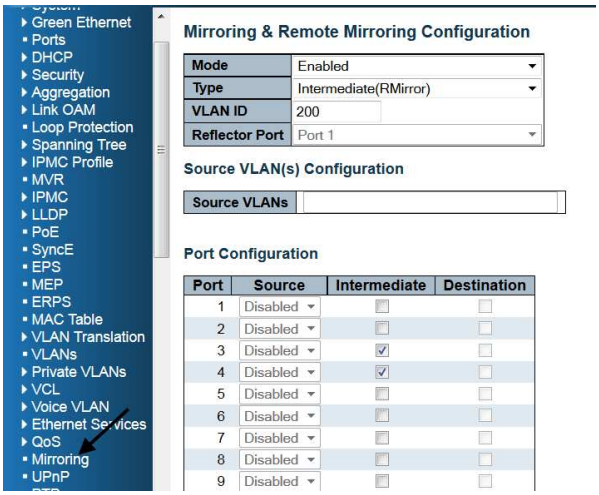
  Note The intermediate port needs to disable MAC Table learning.

- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - intermediate switch configuration

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 intermediate interface GigabitEthernet 1/3-4
(config)# monitor session 1 intermediate remote vlan 200
(config)# interface GigabitEthernet 1/3-4
(config-if)# no mac address-table learning
```

Figure 27. Web GUI: Remote Mirroring - Intermediate Switch



Switch 3

Configure Switch 3 as Destination Switch with the following parameters.

- Intermediate port: 4

  Note The intermediate port needs to disable MAC Table learning.

- Destination port: 1

  Note1 The device only supports one destination port.

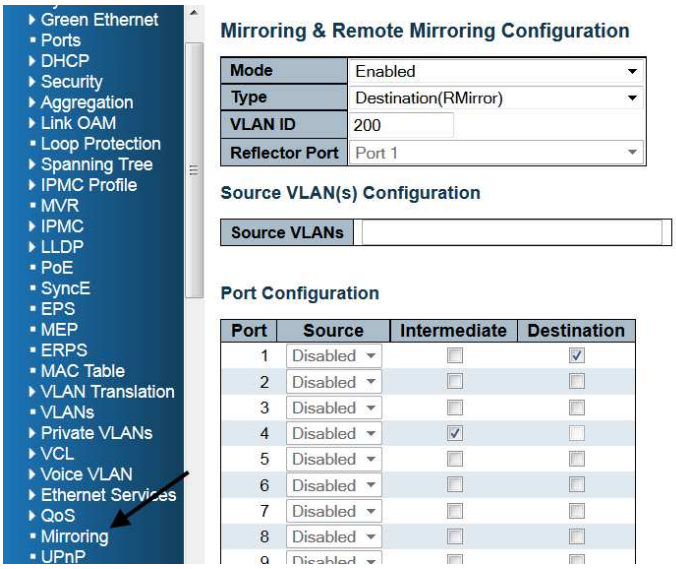
  Note2 The destination port needs to disable MAC Table learning.

- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - destination switch

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 destination interface GigabitEthernet 1/1
(config)# monitor session 1 intermediate interface GigabitEthernet 1/4
(config)# monitor session 1 source remote vlan 200
(config)# interface GigabitEthernet 1/1,4
(config-if)# no mac address-table learning
```

Figure 28. Web GUI: Remote Mirroring - Destination Switch



6.3 Configuration Options

6.3.1 Type

Mirror

Configure the switch to local mirror mode. The source port(s) and destination port are located on the same switch.

Source

Configure the switch as a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.

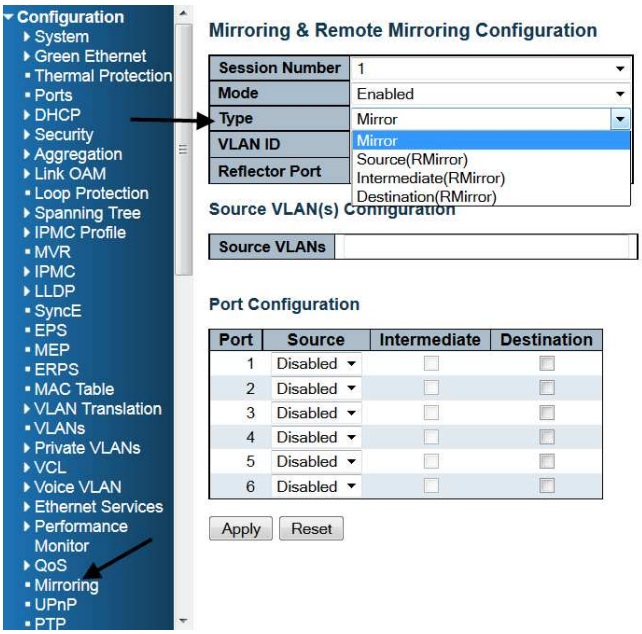
Intermediate

Configure the switch as a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.

Destination

Configure the switch as an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

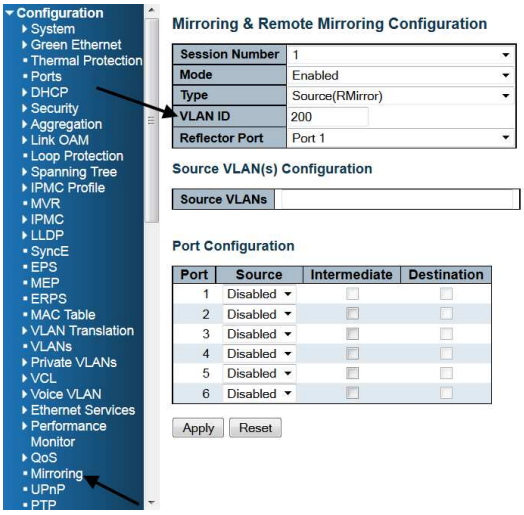
Figure 29. Web GUI: Mirroring Type



6.3.2 VLAN ID

The VLAN ID points out where the monitor packet will copy to. It is recommend to be separate from the VLAN of normal data traffic.

Figure 30. Web GUI: Remote Mirroring - VLAN ID



6.3.3 Reflector Port

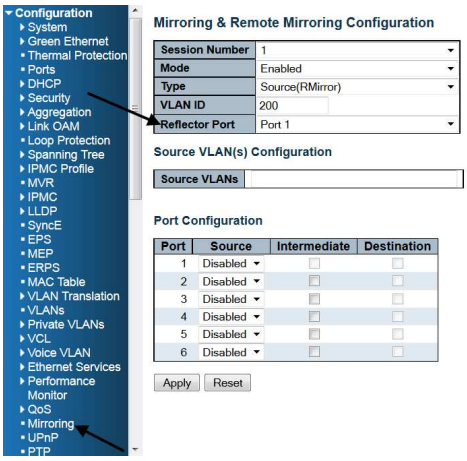
The reflector port is a method to redirect traffic to the Remote Mirroring VLAN. The reflector port will stop working as a normal port if it is configured as a reflector port.

Note1 The reflector port needs to select only on Source switch type.

Note2 The reflector port needs to disable MAC Table learning and STP.

Note3 The reflector port only supports on pure copper ports.

Figure 31. Web GUI: Remote Mirroring Reflector Port

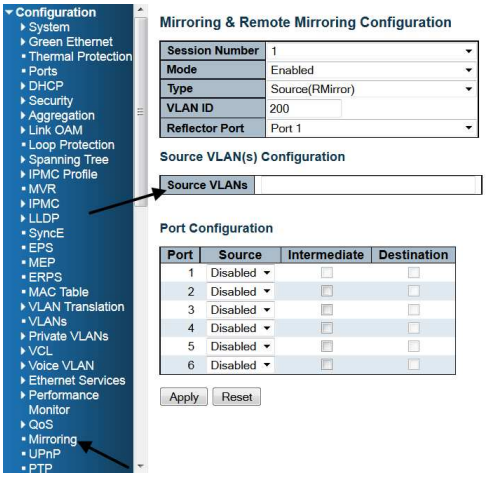


6.3.4 Source VLAN(s) Configuration

The switch can support VLAN-based Mirroring.

Note The mirroring session may have either ports or VLANs as sources, but not both.

Figure 32. Web GUI: Mirroring Source VLAN



6.3.5 Remote Mirroring Port Configuration

Source

- Disabled: Neither frames transmitted nor frames received are mirrored.
- Both: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.

- Rx only: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.
- Tx only: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.

Intermediate

For Remote Mirroring only, the intermediate port is a switched port to connect to other switch.

Note The intermediate port needs to disable MAC Table learning.

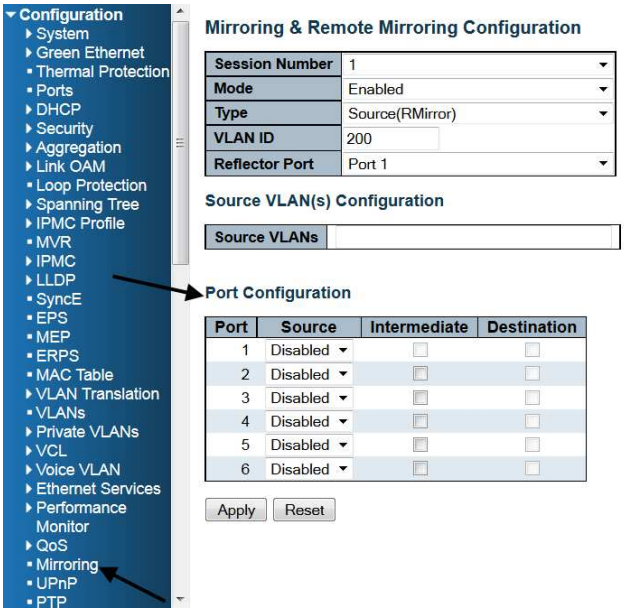
Destination

The destination port is a switched port that you receive a copy of traffic from the source port.

Note1 On mirror mode, the device only supports one destination port.

Note2 The destination port needs to disable MAC Table learning.

Figure 33. Web GUI: Mirroring Port Configuration



6.3.6 Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator needs to check whether or not other features are enabled or disabled. For example, the administrator cannot enable the MSTP on a reflector port. All monitor traffic is blocked on the reflector port.

All recommended settings are described in the below table.

	Impact	Source port	Reflector port	Intermediate port	Destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		

acl	Critical	* disabled	* disabled	* disabled	
dhcp_relay	High	* disabled	* disabled		
dhcp_snooping	High	* disabled	* disabled		
ip_source_guard	Critical	* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical				un-conflict
ipmc/mldsnp	Critical				un-conflict
lacp	Low			o disabled	
lldp	Low			o disabled	
mac learning	Critical	* disabled	* disabled	* disabled	
mstp	Critical	* disabled		o disabled	
mvr	Critical				un-conflict
nas	Critical	* authorized	* authorized	* authorized	
psec	Critical	* disabled	* disabled	* disabled	
qos	Critical	* unlimited	* unlimited	* unlimited	
upnp	Low			o disabled	
mac-based vlan	Critical	* disabled	* disabled		
protocol-based vlan	Critical	* disabled	* disabled		
vlan_translation	Critical	* disabled	* disabled	* disabled	
voice_vlan	Critical	* disabled	* disabled		

Legend:
* -- must
o -- optional
Impact: Critical/High/Low
Critical 5 packets -> 0 packet
High 5 packets -> 4 packets
Low 5 packets -> 6 packets

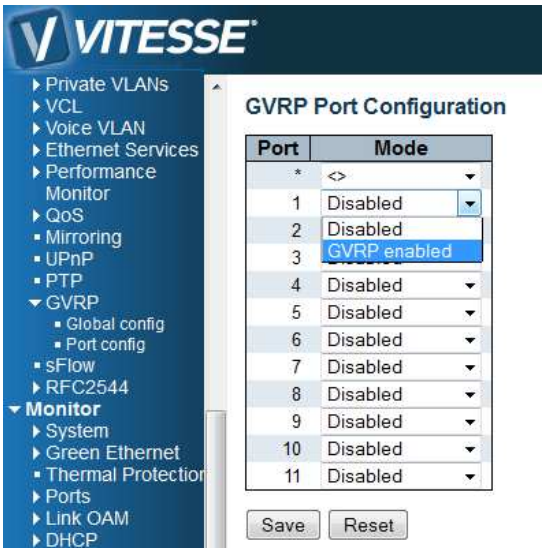
7 GVRP

Generic VLAN registration protocol, or GVRP for short is specified in IEEE 802.1Q-2005, clause 11 and IEEE 802.1D.2004, clause 12.

7.1 GVRP Port Configuration

GVRP is enabled on a port basis in the web GUI under **Configuration** > **GVRP** > **Port config** as shown below.

Figure 34. GVRP Port Configuration



The associated ICLI command is

```
(config-if)# [no] gvrp
```

where the **no** form disables GVRP on that port.

7.2 Special Note for CEService

In general this is enough for GVRP to work, however the CEService SDK allows the user to configure whether a L2CP (Layer 2 Control Protocol) shall be forwarded or peer'ed, meaning sent to the CPU. The default is that it shall be forwarded.

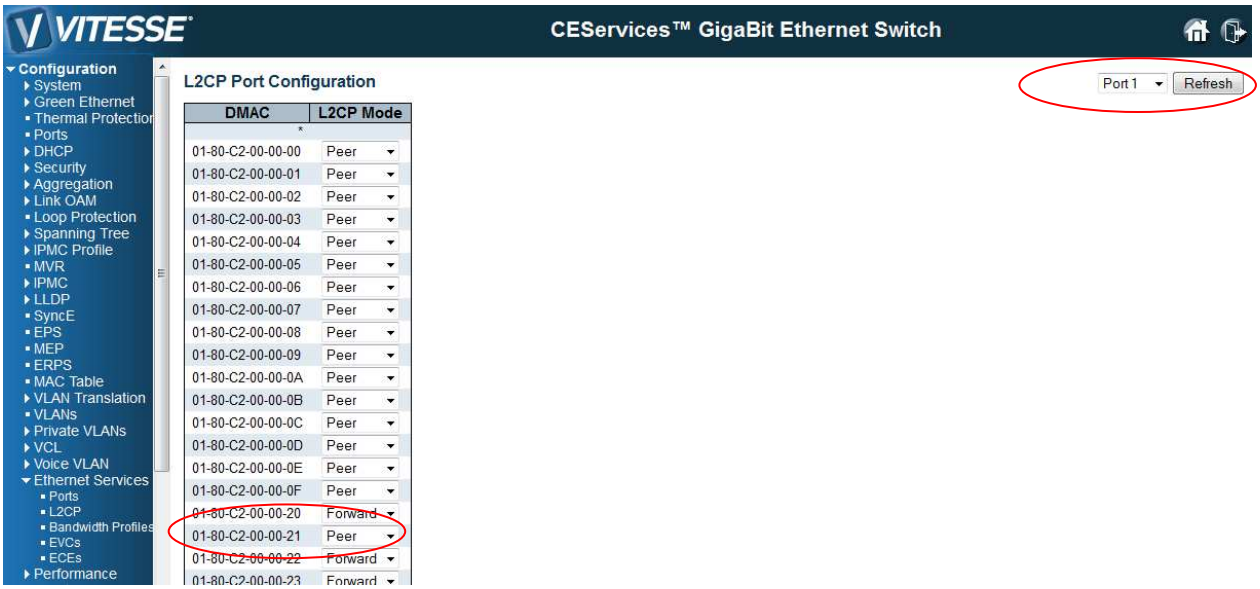
Thus when using CEService, it is not enough to enable GVRP on a port as described above. In addition the system must be told how GARP frames shall be peer'ed as shown below:

```
(config-if)# gvrp
(config-if)# evc l2cp peer 17
```

In this case 17 is the ID for GARP.

The peering of the GARP protocol can also be configured in the web GUI by going into **Configuration** > **Ethernet Services** > **L2CP** and then select the port to configure in the upper right corner.

Figure 35. L2CP Peer Forward



The GARP multicast address is 01-80-c2-00-00-21, and is the 17th entry in the list above, counting from zero.

In general all ports should be configured to peer this multicast address, if the device is supposed to run GVRP at all. For this the command

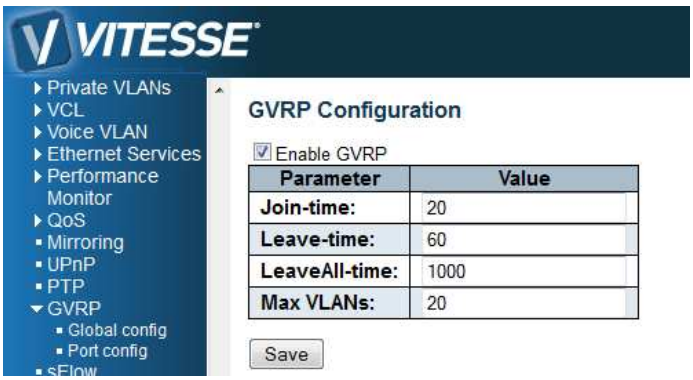
```
(config)# interface *
(config-if)# evc l2cp peer 17
```

would do.

7.3 GVRP Global Configuration

A small number of parameters can be configured for GVRP. These parameters are found in the web GUI under **Configuration** > **GVRP** > **Global config**, as shown below.

Figure 36. GVRP Global Configuration



The Enable GVRP checkbox enables GVRP globally. So GVRP is only turned on, on a port, when GVRP is globally enable and enabled on the port in question. See section 7.1.

The 3 items: *Join-time*, *Leave-time* and *LeaveAll-time* are protocol parameters in units of centi-seconds, (i.e., in 1/100 seconds). These are parameters according to the GARP (IEEE 802.1D-2004, clause 12) standard.

```
(config)# [no] gvrp time join-time 19
(config)# [no] gvrp time leave-time 61
(config)# [no] gvrp time leave-all-time 1234
```

Where the **no** form disables GVRP or put the protocol parameter into its default value. The last 3 commands can be put into a single line.

```
(config)# gvrp time join-time 19 leave-time 61 leave-all-time 1234
```

The last parameter is the number of VLANs that GVRP can administer. This put an upper limit to the number resources that can be used.

When enabling GVRP globally with

```
(config)# [no] gvrp
```

The *Max VLANs* is set to 20. If another value is needed, say 100, then turn GVRP on with the following command.

```
(config)# gvrp max-vlans 100
```

Note GVRP must be disabled in advance for the max-vlan number to be changed.

7.4 The State of GVRP

It is possible to see what state the GVRP protocol is in with the following command.

```
# platform debug allow
#
# debug gvrp protocol-state interface GigabitEthernet 1/* vlan 1-10
             |<-------- State of: ------->||<--- Timer [cs]: -->|
Sw Port VLan  Applicant Registrar LeaveAll  txPDU leave leaveall  GIP-Context
 1    9    1       VO     Fixed     Passive     -    -      137     -
 1    9    2       VO        MT     Passive     -    -      136     -
 1    9    3       VO        MT     Passive     -    -      136     -
 1    9    4       VO        MT     Passive     -    -      135     -
...
 1    9   10       VO        MT     Passive     -    -      132     -
#
```

In this example we say we will see the state for all gigabit port in switch 1 and VLANs in range 1-10. From the output it turns out, that only port 9 was GVRP enabled. Also see that VLAN ID 1 is `Fixed`.

Only ports that are GVRP enabled are shown. So when a command like the one above says, that all gigabit port for switch 1 shall be show, then it will still only be the port for which GVRP has been enabled.

All terms like Applicant, Registrar, … , GIP-Context, can be found in the GARP standard.

A dash for a timer means that, that timer is not running.

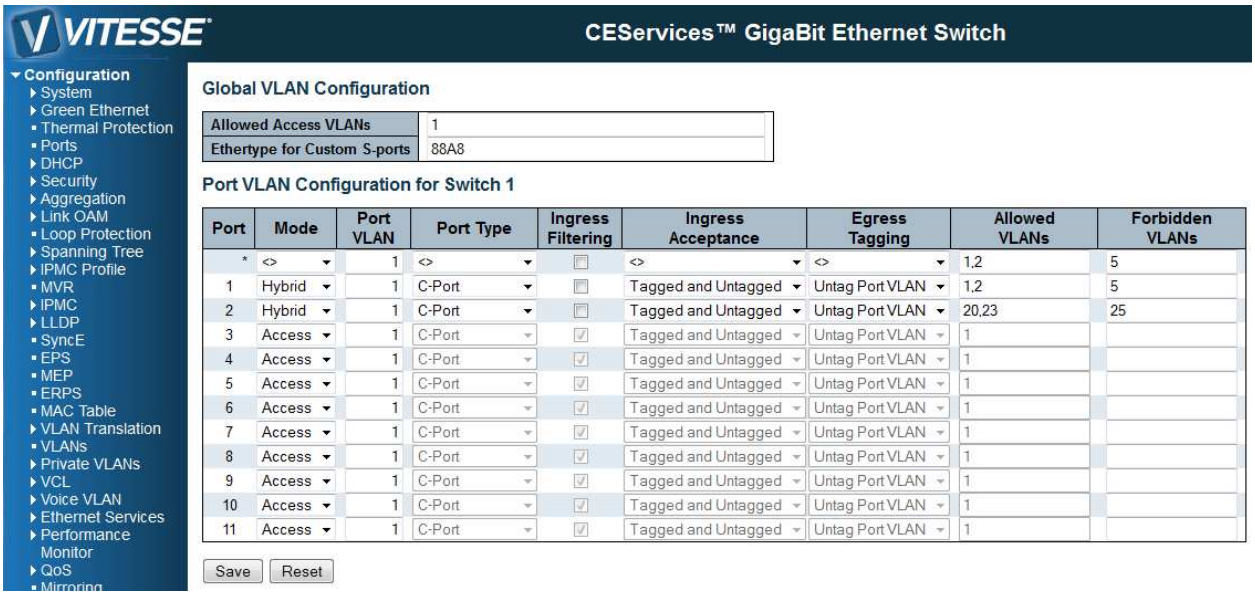
A dash for GIP-Context means that that particular entry is not in a GIP-Context. This will be the case, if the port is down or if it is not in forwarding mode due to spanning tree.

GIP-Context 0 is *Base Spanning Tree Context* (IEEE 802.1D-2004, 12.2.4). If MSTP is used, then GIP-Context 1 is MSTI-1, …, GIP-Context 7 is MSTI-7.

7.5 Fixed and Forbidden VLANs

The Fixed- and Forbidden VLANs are configured from the VLAN menu at **Configuration** > **VLANs**.

Figure 37. VLAN Table



In the VLAN table above VLAN 1 and 2 are set to "Allowed" and VLAN 5 to "Forbidden". Port 2 has different settings.

Note: In GVRP, *Allowed VLANs* are called *fixed* and *Forbidden VLANs* are also called *forbidden*.

With the above configuration, and with port 1, 2 and 3 GVRP enabled, the state of GVRP is:

```
# debug gvrp protocol-state interface GigabitEthernet 1/* vlan 1-30
                |<-------- State of: ------->||<--- Timer [cs]: -->|
Sw Port VLan  Applicant Registrar LeaveAll  txPDU leave leaveall  GIP-Context
 1    1    1       VO      Fixed     Passive      -     -       895      -
 1    1    2       VO      Fixed     Passive      -     -       894      -
 1    1    3       VO         MT     Passive      -     -       894      -
 1    1    4       VO         MT     Passive      -     -       893      -
 1    1    5       VO  Forbidden     Passive      -     -       893      -
 1    1    6       VO  Forbidden     Passive      -     -       892      -
 1    1    7       VO  Forbidden     Passive      -     -       891      -
 1    1    8       VO         MT     Passive      -     -       891      -
 .    .    .        .          .           .      .     .         .      .
 1    1   30       VO         MT     Passive      -     -       877      -
 1    2    1       QA         MT     Passive      -     -       140      0
 1    2    2       VO         MT     Passive      -     -       139      0
 .    .    .        .          .           .      .     .         .      .
 1    2   19       VO         MT     Passive      -     -       129      0
 1    2   20       VO      Fixed     Passive      -     -       128      0
 1    2   21       VO         MT     Passive      -     -       128      0
 1    2   22       VO         MT     Passive      -     -       127      0
 1    2   23       VO      Fixed     Passive      -     -       126      0
 1    2   24       VO         MT     Passive      -     -       126      0
 1    2   25       VO  Forbidden     Passive      -     -       125      0
 1    2   26       VO         MT     Passive      -     -       124      0
 .    .    .        .          .           .      .     .         .      .
 1    2   30       VO         MT     Passive      -     -       122      0
 1    3    1       VO      Fixed     Passive      -     -       743      0
 1    3    2       VO         MT     Passive      -     -       743      0
```

```
 .    .    .       .          .            .      .    .       .      .
1    3   30      VO         MT     Passive      -    -      726      0
#
```

If we focus in the Registrar state, it is seen, that the Fixed and Forbidden states match, what has been set in the VLAN menu.

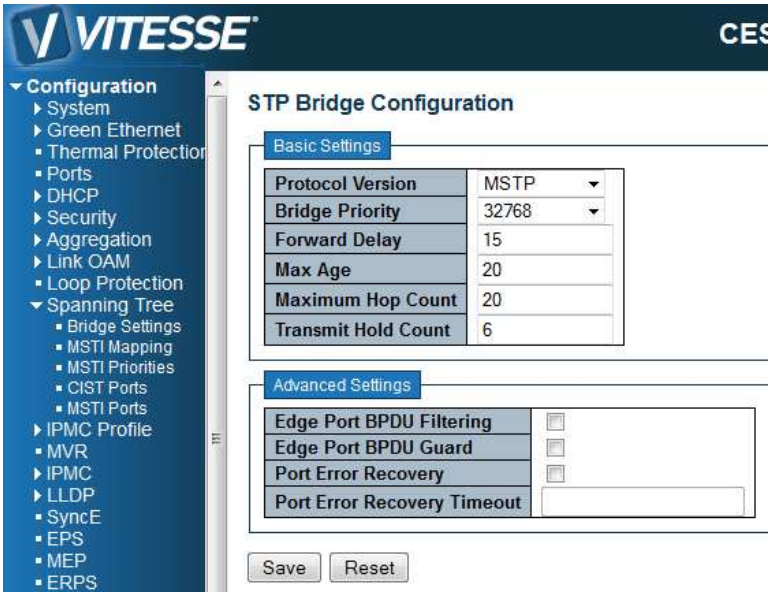
In this context, we have configured 9 VLAN IDs: 1, 2, 5, 6, 7, 20, 23, and 25. This takes 9 GVRP resources. By default we have 20 GVRP resources. If the *Allowed VLANs* are set to 1-4095, which is default when setting the Mode to Hybrid, and that port is GVRP enabled, then it would require 4096 GVRP resources. So in that case, the GVRP should have been started with the following command.

```
(config)# gvrp max-vlans 4096
```

8 Multiple Spanning Tree Protocol

8.1 Bridge Settings

Figure 38. Bridge Setting



8.1.1 ICLI Commands for Basic Settings

The following ICLI commands refer to the Basic Settings section in Figure 38.

The *protocol version* is set by the ICLI command:

```
(config)# spanning-tree mode [mstp|rstp|stp]
```

The *bridge priority* is set by:

```
(config)# spanning-tree mst 0 <4096*i, i=0,…,15>
```

where <4096*i, i=0,…,15> is one of the numbers 4096*i, where i=0,…,15.

The *forward delay* is set by:

```
(config)# spanning-tree mst forward-time <4-30>
```

Where <4-30> is one of the numbers 4, 5,…,30.

The *max age* is set by:

```
(config)# spanning-tree mst max-age <6-40>
```

The *max hop* is set by:

```
(config)# spanning-tree mst max-hop <6-40>
```

The *transmit hold count* is set by:

```
(config)# spanning-tree transmit hold-count <1-10>
```

8.1.2 ICLI Commands for Advanced Settings

The following ICLI commands refer to the Advanced Settings section in Figure 38.

The *edge port BPDU filtering* is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-filter
```

The *edge port BPDU guard* is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-guard
```

The *port error recovery* and *port error recovery timout* is set by one ICLI command:

```
(config)# [no] spanning-tree recovery interval <30-86400>
```

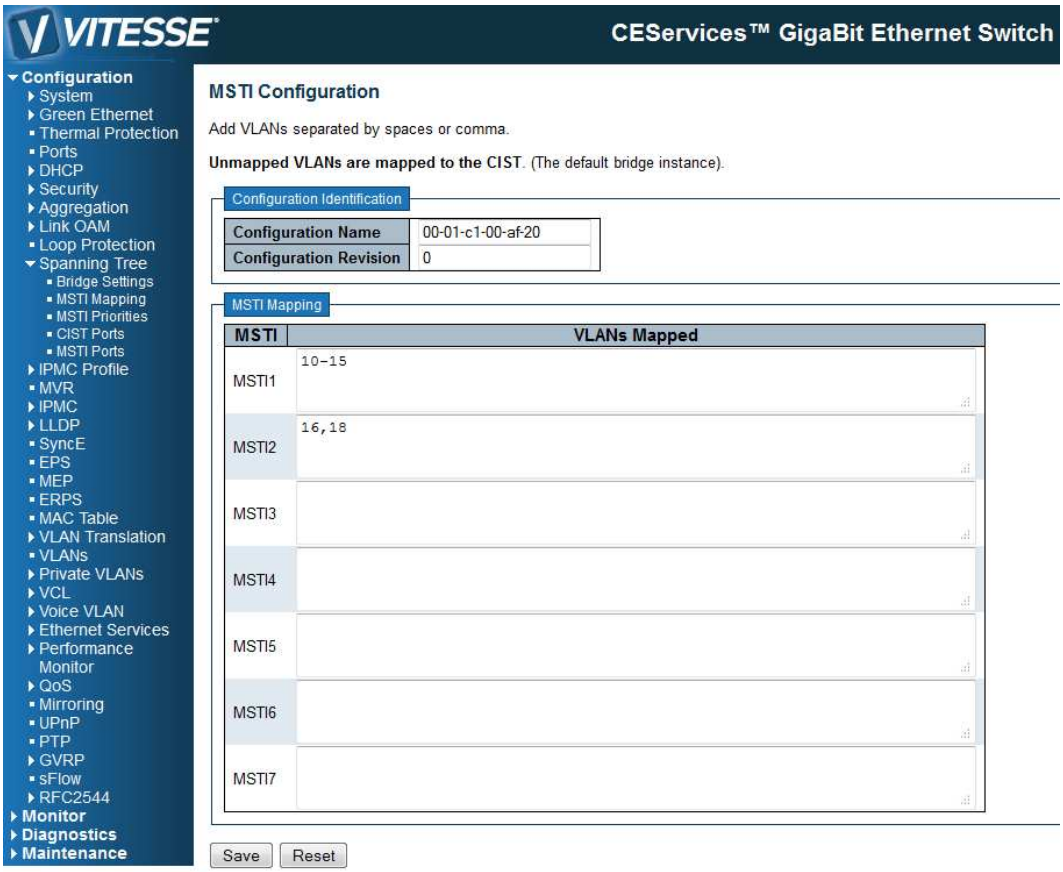
which both enables and set the value. The **no** form disables it.

8.2 MSTI Configuration

By default, all VLAN Ids are mapped to the Common and Internal Spanning Tree (CIST). If the protocol version is set to MSTP, then a VLAN ID can be mapped to one out of 8 spanning trees, where CIST is one. The 7 others are called MSTI1,…, MSTI7 as shown in Figure 39. A MSTI configuration also has a name and a revision as the figure shows.

All these values have to be configures identical on the switches in the network. Otherwise the configuration will not take effect.

Figure 39. MSTI Configuration



The configuration identity is configured with:

```
(config)# spanning-tree mst name <ConfigurationName> revision <RevisionNumber>
```

where <ConfigurationName> is a string of maximum length 32 characters, and <RevisionNumber> is an integer in the range 1,…,65535.

In the above example, the VLANs are added to MSTI1 and MIST2 with the commands:

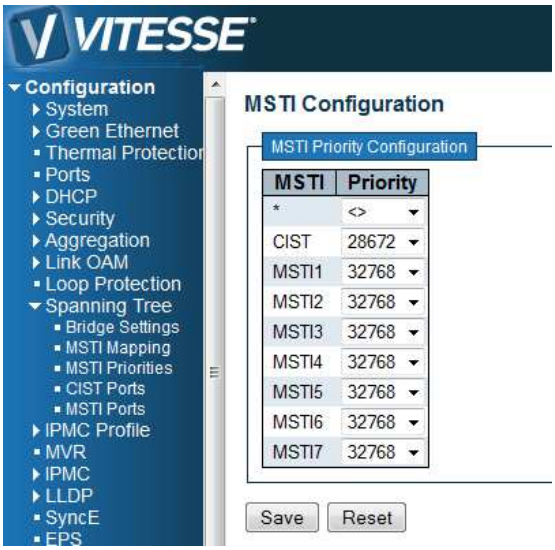
```
(config)# [no] spanning-tree mst 1 vlan 10-15
(config)# [no] spanning-tree mst 2 vlan 16,18
```

The **no** form deletes all VLANs in the msti in question.

8.3 MSTI Priorities

Each MSTI and CIST can be given a priority as show below:

Figure 40. MSTI Priorities



A low priority number means higher priority.

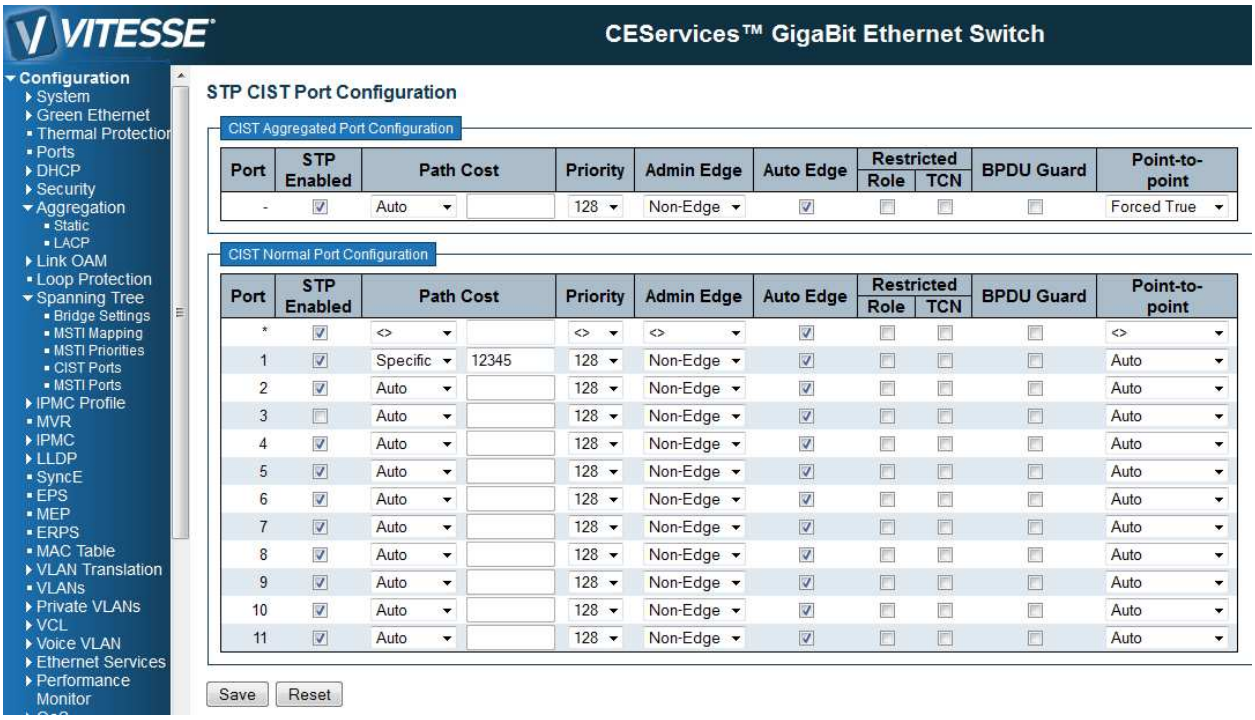
A *Bridge Identifier* is constructed per CIST, MSTI1,…,MSTI7, which is the Bridge Priority, see Figure 38, plus the number in the figure above. This is concatenated with the MAC address of the switch. In this way the Bridge Identifier should be unique.

A low Bridge Identifier means a higher priority. A high priority means that the switch tends to be the root of the spanning tree in favor of switched with lower priority. So if two switches have the same Bridge Priority, then for example, by setting MSTI1's priority higher on the one switch than the other, and vice versa with MSTI2, the one switch tends to be root of the one MSTI and the other switch for the other MSTI.

8.4 STP CIST Port Configuration

Configurations concerning STP on a port basis are configured in the web GUI at **Configuration** > **Spanning Tree** > **CIST Ports**, as shown in Figure 41.

Figure 41. CIST Port Configuration



It is important for the user to understand that all parameters above, except *Path Cost* and *Priority*, are specific for the port and not for CIST. As will be seen in section 8.5, these two parameters can be set for each MSTI. But all the other parameters cannot, because they apply to the port. If for example spanning tree is disabled (as it is for port 3), then this goes for the CIST and all the MSTIs.

When using the ICLI, the *CIST Aggregation Port Configuration* commands are performed at the *Config* mode prompt as seen below.

```
(config)#
```

The *CIST Normal Port Configuration* commands are performed in the *Config Interface* mode prompt as seen below.

```
(config-if)#
```

The commands described below assume that the user is in the interface config mode.

8.4.1 STP Enabled

A port can be individually enabled or disabled for taking part in the spanning tree protocol with the following command.

```
(config-if)# [no] spanning-tree
```

8.4.2 Path Cost and Priority

The path cost and priority are set by the following commands:

```
(config-if)# spanning-tree mst 0 cost <Cost>
(config-if)# spanning-tree mst 0 port-priority <Priority>
```

where <Cost> is a number in the range 1 to 200000000 or it may be auto. If set to auto, then the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

The <Priority> is a number in the range 0 to 240 and a multiple of 16. Note that if it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. If two ports have the same cost, then priority is used as a tie breaker.

8.4.3 Admin Edge and Auto Edge

These two features are turned on and off by the following ICLI commands:

```
(config-if)# [no] spanning-tree edge
(config-if)# [no] spanning-tree auto-edge
```

The first command changes the field *Admin Edge* in the web GUI, and the second changes *Auto Edge*. These two values control how a port is declared to be an edge port or not. An edge port is a port which is not connected to a bridge.

If auto edge is enabled, then the port determines whether it is an edge port by registering if BPDUs are received on that port. The admin edge determines what the port should start as, being edge or not, until auto edge if enabled, then change.

The decision can be seen by selecting **Monitor** > **Spanning Tree** > **Bridge Status**, then clicking on CIST. Then the *Edge* field shows the decision.

8.4.4 Restricted Role and Restricted TCN

These two features are turned on and off by the following ICLI commands:

```
(config-if)# [no] spanning-tree restricted-role
(config-if)# [no] spanning-tree restricted-tcn
```

If restricted role is enabled it causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network to influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

If restricted TCN is enabled it causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

8.4.5 BPDU Guard

This feature is turned on by the following ICLI commands:

```
(config-if)# [no] spanning-tree bpdu-guard
```

If enabled it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting.

8.4.6 Point-to-point

This feature is turned on by the following ICLI commands:

```
(config-if)# [no] spanning-tree link-type {auto|point-to-point|shared}
```

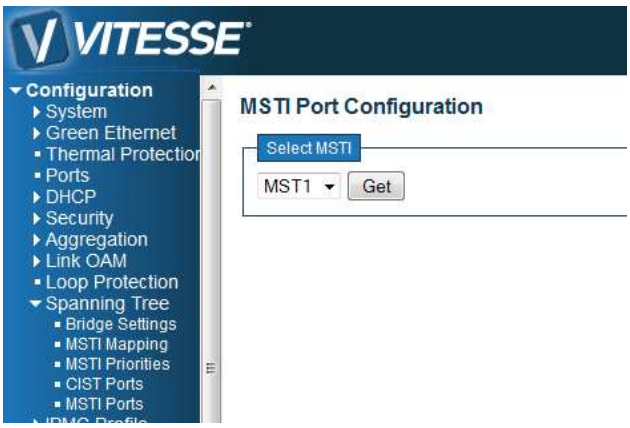
where the **no** form is equivalent to setting it to `auto`.

Setting the link to point-to-point, shows up in the web GUI as *Forced True*. Setting it to shared, is shown as *Force False*. Setting it to auto shows as *Auto*.

8.5 MSTI Ports

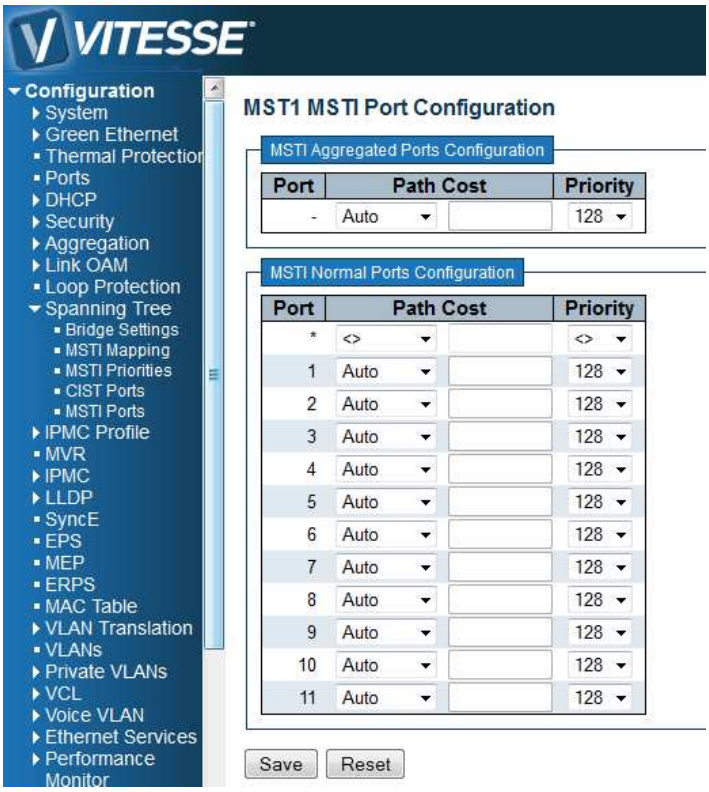
The user must select which MSTI configuration to view starting at **Configuration** > **Spanning Tree** > **MSTI Ports** as shown below.

Figure 42. MSTI Port Configuration



Select the desired MSTI and press **Get**.

Figure 43. MST1 MSTI Port Configuration



The ICLI commands for setting the Path cost and Priority, is the same as for CIST, as described in section 8.4, but with the change that the msti is not 0 (MSTI0 is CIST), but a number from 1 to 7.

```
(config-if)# spanning-tree mst <MSTI> cost <Cost>
(config-if)# spanning-tree mst <MSTI> port-priority <Priority>
```

Here `<MSTI>` is the number of the msti, from 1 to 7.

The other parameters are the same as in the CIST case but are repeated anyway.

The `<Cost>` is a number in the range 1 to 200000000 or it may be `auto`. If set to `auto`, then the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

The `<Priority>` is a number in the range 0 to 240 and a multiple of 16. Note that if it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. And if two ports have the same cost, then priority is used as a tie breaker.