

Vubiq HaulPass V10g User Manual



10g



Making Millimeter Wave Ubiquitous

Vubiq Networks, Inc. (“Vubiq”) retains the right to make changes to its products or specifications to improve performance, reliability or manufacturability. All information in this document, including descriptions of features, functions, performance, technical specifications and availability, is subject to change without notice at any time. While the information furnished herein is held to be accurate and reliable, no responsibility will be assumed by Vubiq for its use. Furthermore, the information contained herein does not convey to the purchaser of microelectronic devices any license under the patent right of any manufacturer.

Vubiq products are not intended for use in products or applications, including, but not limited to, medical devices (including life support and implantable medical devices), nuclear products, or other safety-critical uses where failure of a Vubiq product could reasonably be expected to result in personal injury or death. Anyone using a Vubiq product in such an application without express written consent of an officer of Vubiq does so at their own risk, and agrees to fully indemnify Vubiq for any damages that may result from such use or sale.

© 2018 Vubiq Networks, Inc. All rights reserved. HaulPass V10g is a trademark of Vubiq Networks, Inc. All other products or service names used in this publication are for identification purposes only, and may be trademarks or registered trademarks of their respective companies. All other trademarks or registered trademarks mentioned herein are the property of their respective holders.

TABLE OF CONTENTS

1.0 Important Information	7
1.1 Cautions and Warnings	7
1.2 Observe Standard Precautions	7
1.3 Qualified Personnel	7
1.4 Service	7
1.5 Regulatory Information	7
North America.....	7
47 CFR Part 15.....	8
Industry Canada RS210 Issue 8.....	8
RF Exposure Summary	8
ISED 9	
Protection Against Interference	9
1.6 Warranty Information.....	9
1.7 Contacting Vubiq Networks, Inc.	9
2.0 Introduction	10
2.1 Shipping Content.....	10
2.2 The HaulPass V10g	11
3.0 Installation Instructions	13
3.1 Operating Modes.....	13
3.2 Unpacking the HaulPass V10g.....	13
3.3 Hardware Installation.....	14
3.4 Alignment	16
3.5 HaulPass V10g Ports	18
3.6 Power over Ethernet++ Modules	18
3.7 Lightning/Surge Protection	19
3.8 Grounding.....	19
4.0 Alignment Details	20
4.1 HaulPass V10g Throughput	20
4.2 Alignment Procedure.....	20
4.3 Mean Squared Error (MSE).....	21
5.0 Additional Instructions	22
5.1 Changing from 10 Gbps/10000Base to 2.5 Gbps/1000Base.....	22
Changing the Mode via the Webpage.....	22
Changing the Mode via the CLI	22
5.2 Changing the IPv4 Address.....	23
Changing the Address via the Webpage	23
Changing the Address via the CLI	24
5.3 Using the 48VDC Power Port	24
5.4 Upgrading the Firmware	25
Upgrading the RF Firmware	25
Upgrading the Network Switch Firmware.....	25
5.5 Changing the Clock Time	26

Configuring the Network	26
Pointing to the NIST Internet Time Servers	26
Configuring the Local Time Zone.....	27
Saving the Configuration	28
5.6 Setting https Web Access.....	29
5.7 Restoring to Factory Default IP Address and Password.....	31
Manual Process.....	31
GUI Process	32
6.0 MAC Address Table	33
6.1 Setting the Aging Time.....	33
6.2 Adding a Static MAC Address Entry.....	34
6.3 Showing the MAC Address Table	34
7.0 VLAN.....	36
7.1 VLAN Quick Configuration Example.....	36
7.2 Global Configuration.....	37
Existing VLAN.....	37
VLAN Naming.....	38
Ethertype for Custom S-ports	38
7.3 Port-based Configuration.....	39
Port Mode 39	
Port VLAN40	
Port Type 41	
Ingress Filtering	43
Ingress Acceptance	43
Tagged and Untagged	43
Tagged Only	43
Untagged Only.....	43
Egress Tagging.....	44
Allowed VLANs	45
Forbidden VLANs	46
8.0 Generic VLAN Registration Protocol	48
8.1 GVRP Port Configuration	48
8.2 Special Note for CEService	49
8.3 GVRP Global Configuration	50
8.4 Fixed and Forbidden VLANs	51
9.0 Multiple Spanning Tree Protocol.....	52
9.1 Bridge Settings	52
ICLI Commands for Basic Settings.....	52
ICLI Commands for Advanced Settings.....	52
9.2 MSTI Configuration	53
9.3 MSTI Priorities	54
9.4 STP CIST Port Configuration	54

- STP Enabled 55
- Path Cost and Priority 55
- Admin Edge and Auto Edge 55
- Restricted Role and Restricted TCN 55
- BPDU Guard..... 56
- Point-to-Point..... 56
- 9.5 MSTI Ports 56
- 10.0 RF Commands 58**
- 10.1 RF Board (Board Setting/Status)..... 58
 - current-5v (Board 5V current status)..... 58
 - firmware version (Board firmware version setting)..... 58
 - fpga (Board FPGA version setting)..... 59
 - temp (Board temperature setting)..... 60
 - uptime (Board uptime status)..... 60
- 10.2 rf rx (Rx Module Command) 60
 - auto-atten (Rx auto-atten setting/status)..... 61
 - bb atten (Rx BB atten setting)..... 61
 - dssi (Rx DSSI status)..... 61
 - freq (Rx frequency setting (GHz)) 63
 - if (Rx IF atten setting) 64
 - sync (Rx sync status)..... 65
 - synth (Rx synth status) 65
 - temp (Rx temperature setting) 66
- 10.3 rf tx (RF Tx Module Setting/Status) 67
 - freq (Tx frequency setting (GHz)) 67
 - if (Tx IF atten setting)..... 67
 - synth (Tx synth status)..... 68
 - temp (Tx temperature setting) 69

LIST OF TABLES

- Table 1. HaulPass V10g Specifications 12
- Table 2. V10g Expected Throughput and Expected LEDs..... 20

LIST OF FIGURES

- Figure 1. HaulPass V10g Packaging 13
- Figure 2. L-Com Lightning Arrestor (Front View) 14
- Figure 3. L-Com Lightning Arrestor (Rear View) 14
- Figure 4. Pole Mount Bracket Assembly 15
- Figure 5. Mount the V10g Terminal (Front View) 15
- Figure 6. Mount the V10g Terminal (Rear View)..... 16
- Figure 7. Scope Mount and Scope 16
- Figure 8. LED Status..... 17
- Figure 9. HaulPass V10g Ports..... 18
- Figure 10. HaulPass V10g Throughput, Modulation and Profile Graph 20
- Figure 11. Connecting the 48VDC Power Port 24
- Figure 12. Restoring the V10g to Factory Default IP Address and Password..... 31

Figure 13. Change the Aging Time to 600 Seconds	33
Figure 14. Static MAC Address Configuration	34
Figure 15. MAC Address Table.....	35
Figure 16. Default VLAN Configuration.....	36
Figure 17. Creating VLAN 2.....	36
Figure 18. Setting the Trunk Port.....	37
Figure 19. VLAN Allowed Access VLANs Configuration	38
Figure 20. VLAN Ethertype for Custom S-ports Configuration.....	39
Figure 21. VLAN Mode Configuration	40
Figure 22. VLAN PVID Configuration (Access).....	41
Figure 23. VLAN PVID Configuration (Hybrid).....	41
Figure 24. VLAN Port Type Configuration.....	42
Figure 25. VLAN Ingress Filtering Configuration.....	43
Figure 26. VLAN Ingress Acceptance Configuration.....	44
Figure 27. VLAN Egress Tagging Configuration	45
Figure 28. Allowed VLANs Configuration (Trunk)	45
Figure 29. Allowed VLANs Configuration (Hybrid)	46
Figure 30. Forbidden VLANs Configuration	47
Figure 31. GVRP Port Configuration.....	48
Figure 32. L2CP Peer Forward	49
Figure 33. GVRP Global Configuration	50
Figure 34. VLAN Table	51
Figure 35. Bridge Setting	52
Figure 36. MSTI Configuration.....	53
Figure 37. MSTI Priority Configuration.....	54
Figure 38. STP CIST Port Configuration.....	54
Figure 39. MSTI Port Configuration	56
Figure 40. MST1 MSTI Port Configuration.....	57

1.0 Important Information

Note: Changes or modifications of the system not expressly approved by Vubiq Networks, Inc. could void the user's authority to operate the equipment.

1.1 Cautions and Warnings

The following symbol is used in this manual to indicate that the installer should take particular caution to prevent injury or damage to the equipment.



Exercise caution when you see this symbol. It indicates actions that could be harmful to the installer or to the equipment.

Note: There are no user serviceable parts within the unit and the system should not be opened in the field.

1.2 Observe Standard Precautions

All persons having access to this equipment must observe all standard precautions as defined in applicable national statutory health and safety legislation.

The outdoor equipment must be properly protected against voltage surges and prevent the build-up of static electric charges. We recommend following the IEC 61024 / IEC 62305 standards for proper lightning protection.

For installation in the United States of America, for information with respect to proper grounding and applicable lightning protection for DC cables please refer to Articles 810830 of the National Electrical Code, ANSI / NFPA No. 70.

In cases where the system is installed in a country other than the United States of America, implement protection in accordance with local safety standards and regulatory requirements.

Do not install or operate this equipment in the presence of or close to flammable gases or fumes. Operation of any electrical equipment in such an environment constitutes a potential safety hazard.

1.3 Qualified Personnel

Qualified personnel who understand and are trained to work with the equipment must perform all repair, modification, reconfiguration, and upgrading operations.

Note: Always power the system down before moving or removing the system.

1.4 Service

There are no serviceable parts within the radio units. Only factory trained personnel can provide service on any internal components of the radio units.

1.5 Regulatory Information

North America


These devices have been type approved by FCC in accordance with 47 CFR PART 15.255 of the Federal Communication Commission rules and Industry Canada RSS-210 Issue 8.

No license is required in the U.S. or Canada for millimeter wave radio transmission operating in the 57 –71 GHz frequency band. Customers in other countries are responsible for obtaining proper operator licenses in case they are required by law.

47 CFR Part 15

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.



Making V-Band Ubiquitous

FCC Supplier's Declaration of Conformity

September 17, 2018


This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

According to the Federal Communications Commission the conformity of a device to the requirements shall be certified by a Supplier's "Declaration of Conformity", issued by the party responsible for ensuring compliance. This declaration is satisfied with this document.

Product Name and model number: Vubiq HaulPass V10g, 2ADJ9-V10G-H
Responsible Party located in the United States:


Michael G. Pettus
Vubiq Networks, Inc.
9231 Irvine Blvd
Irvine, CA 92618
(949) 226-8482

Thank you,



Michael G. Pettus
CTO Vubiq Networks, Inc.

Vubiq Networks, Inc. • 9231 Irvine Blvd, Irvine, California 92618 USA • www.vubiqnetworks.com



Making V-Band Ubiquitous

FCC Supplier's Declaration of Conformity

September 17, 2018


This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

According to the Federal Communications Commission the conformity of a device to the requirements shall be certified by a Supplier's "Declaration of Conformity", issued by the party responsible for ensuring compliance. This declaration is satisfied with this document.

Product Name and model number: Vubiq HaulPass V10g, 2ADJ9-V10G-L
Responsible Party located in the United States:

Michael G. Pettus
Vubiq Networks, Inc.
9231 Irvine Blvd
Irvine, CA 92618
(949) 226-8482

Thank you,



Michael G. Pettus
CTO Vubiq Networks, Inc.

Vubiq Networks, Inc. • 9231 Irvine Blvd, Irvine, California 92618 USA • www.vubiqnetworks.com

Industry Canada RS210 Issue 8

This class 1 digital apparatus complies with the Canadian RSS-210 regulation.

Cet appareil de la classe 1 est conforme à la norme RSS-210 du Canada.

RF Exposure Summary

To comply with the FCC / IC RF exposure limits, the device must be installed so as to maintain the minimum separation distance of 2 m (6.6 feet) between the main lobe of the transmit antenna (front of the unit) and nearby persons.

Pour se conformer aux limites d'exposition aux RF de RS-102, Issue 5, la distance minimale de separation entre la principale source d'émission (avant de l'antenne) et des personnes à proximate droit être limité à 2 m (6.6 feet).

ISED

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient un ou des émetteur(s)/récepteur(s) exempt(s) de licence qui sont conformes aux flux RSS exempts de licence d'Innovation, Sciences et Développement économique Canada. Le fonctionnement est soumis aux deux conditions suivantes:

3. Cet appareil ne doit pas causer d'interférences.
4. Cet appareil doit accepter toute interférence, y compris les interférences pouvant entraîner un fonctionnement indésirable de l'appareil.

Protection Against Interference

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation distance between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

1.6 Warranty Information

Vubiq Networks, Inc. warrants this product against faulty materials or workmanship under the terms of a Standard Warranty provided that the product was purchased directly from Vubiq Networks, Inc. or from one of our authorized resellers. Please contact Vubiq Networks, Inc. Customer Service for additional information or to obtain a copy of the Warranty Agreement.

1.7 Contacting Vubiq Networks, Inc.

Corporate Office
9231 Irvine Blvd.
Irvine, California 92618
USA

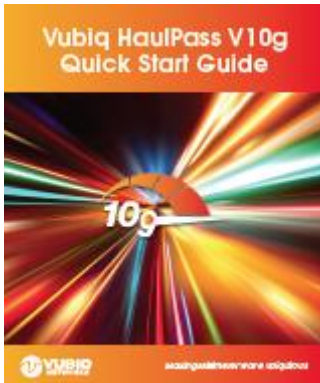
Phone: (949) 226-7185
Website: www.vubiqnetworks.com
E-mail: info@vubiqnetworks.com
Twitter: @vubiqnetworks

2.0 Introduction

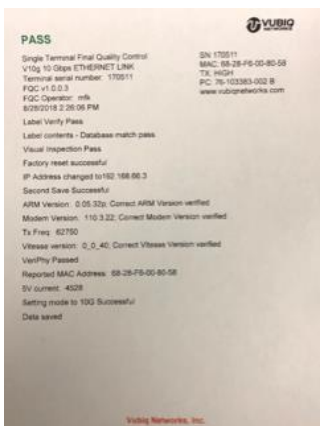
2.1 Shipping Content

The Vubiq Networks, Inc. HaulPass V10g Link ships in two boxes. Each box contains a single terminal and an installation kit. Please verify that each box contains the following items:

- Vubiq HaulPass V10g Quick Start Guide



- Vubiq HaulPass V10g Final Quality Check report



- Vubiq HaulPass V10g terminal



- Vubiq HaulPass Pole Mounting Bracket kit
- Vubiq HaulPass Alignment Scope kit
- Microsemi POE++ and AC Power Cord
- 6' Outdoor Shielded Ethernet cable with V10g Gland
- Bag with 4 V10g Cable Glands, 2 V10g Gland extensions, and a DC Power connector
- Pole Mount L-Com Lightning Arrestor



2.2 The HaulPass V10g

The Vubiq HaulPass V10g is an advanced V-Band millimeter wave radio link that delivers high-speed, low-latency, full-duplex wireless data communications. The flexible V10g operates in two modes:

- 2 x 1.25 Gbps Ethernet connectivity incorporating a fully integrated Ethernet switch (2.5 Gbps aggregate throughput)
- 10 Gbps direct fiber-to-radio connectivity for maximum throughput and minimum latency

Housed in a small, lightweight enclosure that is easy to deploy, the V10g utilizes the license-free V-Band spectrum to cost-effectively meet the ever-expanding needs of today's bandwidth-hungry networks. It provides 500 MHz to 2 GHz channel bandwidth, advanced intelligence, and comprehensive Ethernet switching functionality. Integrated low-latency forward error correction (< 50 μ s) assures data transmission reliability. Line-of-sight wireless connections can span up to 1.8 kilometers (over one mile).

Weighing only 3.8 kg (8.4 lbs) and designed for extreme weather operation, the HaulPass V10g features a ruggedized outdoor enclosure with a compact diameter of only 24.6 cm (9.7"). The V10g can be powered via PoE++ or via a separate auxiliary 48 VDC input, requiring less than 35 watts.

Table 1. HaulPass V10g Specifications

Feature	Specification
Carrier Frequencies	<ul style="list-style-type: none"> License-free V-Band (TX Low 58.00 GHz, TX High 62.75 GHz)
Channel Bandwidth	<ul style="list-style-type: none"> 100 MHz to 2 GHz (baud rate, coding, and modulation programmable)
Modulation	<ul style="list-style-type: none"> BPSK, QPSK, 8PSK, 16QAM, 32QAM, 64QAM, and 128QAM
Throughput	<ul style="list-style-type: none"> 328 Mbps to 10 Gbps, adaptive (hitless)
Transmit Power	<ul style="list-style-type: none"> +15 dBm maximum
Receive Noise Figure	<ul style="list-style-type: none"> 8 dB
Antenna Gain	<ul style="list-style-type: none"> 38.5 dBi
Antenna Beamwidth	<ul style="list-style-type: none"> 1.8° at -3 dB
FEC	<ul style="list-style-type: none"> LDPC
Overall Latency	<ul style="list-style-type: none"> <50 μs
Status LEDs	<ul style="list-style-type: none"> 7 RGB bar-graph layout, programmable functions
Network Interfaces	<ul style="list-style-type: none"> Full Duplex: 1000BASE-T RJ45 (2) (2.5 Gbps aggregate), 1000BASE-X SFP, 10000BASE-X SFP+ (10 Gbps) Auto-negotiation, MDI/MDI-X Address learning, aging and lookup Jumbo frame support to 10K
Carrier Ethernet Options*	<ul style="list-style-type: none"> Feature-rich CE networking with quality of service (QoS), VLAN, MPLS-TP, Policers, MEF CE 2.0 compliant TCAM-based QoS classification L2 switching/L2 multicast
Network Topologies*	<ul style="list-style-type: none"> Ring, daisy chain, mesh
Network Management*	<ul style="list-style-type: none"> HTTP web server with GUI client Command line interface (CLI) Simple Network Management Protocol (SNMP) v 2.0 with private MIB and radio MIB
Software Features	<ul style="list-style-type: none"> Enhanced Intelligent Automatic Gain Control (AGC) Digital Signal Strength Indicator (DSSI) Adaptive coding, modulation, baud rate (ACMB hitless)
Link Range	<ul style="list-style-type: none"> Up to 1.8 km (over one mile), throughput dependent
Power Requirements	<ul style="list-style-type: none"> Low power consumption: 35 watts, PoE++ on RJ45 Port 1, or auxiliary power input at 48 VDC
Weight	<ul style="list-style-type: none"> Light weight: 3 kg (6.6 lbs), not including mounting bracket
Dimensions	<ul style="list-style-type: none"> Small footprint: 24.6 cm (9.7") upper diameter, 27.4 cm (10.8") height, 6.4 cm (2.5") depth
Water/Dust Ingress	<ul style="list-style-type: none"> IP67
Operating Temperature	<ul style="list-style-type: none"> -40°C to 55°C (-40°F to 130°F)

3.0 Installation Instructions

3.1 Operating Modes

The HaulPass V10g units ship ready to operate in 10 Gbps mode. To operate the 1000Base-T or 1000Base-X ports, refer to Section 5.1 to switch the units to 2.5 Gbps mode and enable the internal switch.

The management unit is available through the 1000Base ports in either 10 Gbps or 2.5 Gbps mode at 198.166.68.2 for the TX Low and 198.166.68.3 for the TX High. In 10 Gbps mode, the port traffic in the 1000Base ports is not transmitted over the RF link. To change the address of the management unit, refer to Section 5.2.

Note: After installation, periodically check the Vubiq Networks website at <https://tinyurl.com/vubiqfw> to see if there is a firmware update available. If there is an update available, it should be installed. Refer to Section 5.4.

3.2 Unpacking the HaulPass V10g

Each terminal ships in a separate box. All contents of the terminal kit will be in each box. Upon opening, please inspect the final quality control document and Quick Start Guide prior to continuing. Remove the top foam insert to access the V10g terminal. The remaining accessories are underneath the V10g foam insert (See Figure 1).

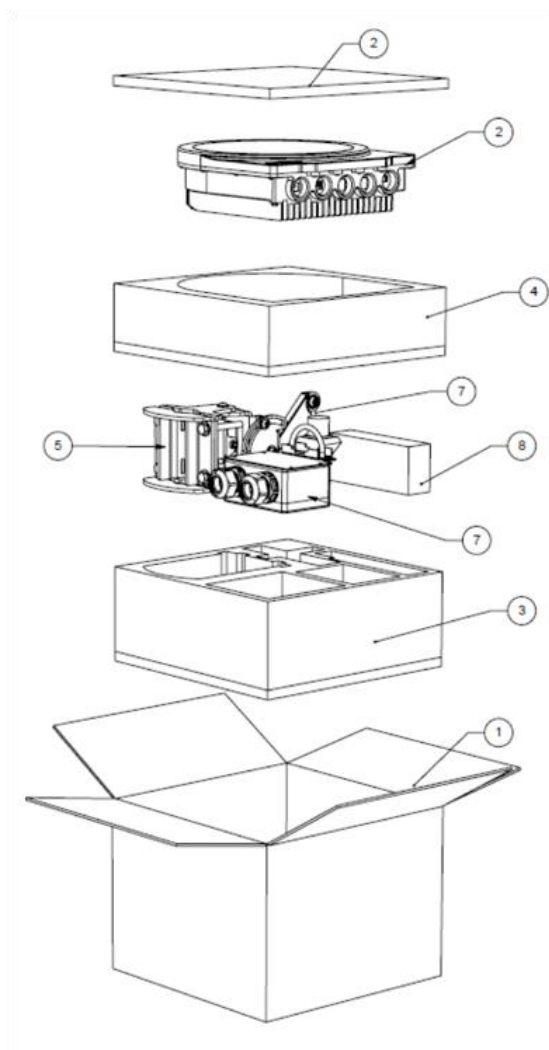


Figure 1. HaulPass V10g Packaging

3.3 Hardware Installation

Step 1. Mount the L-Com Lightning Arrestor to the pole below the mounting point and within 4 feet (1.2 meters) of the V10g Terminal (see Figures 2 and 3).



Figure 2. L-Com Lightning Arrestor (Front View)

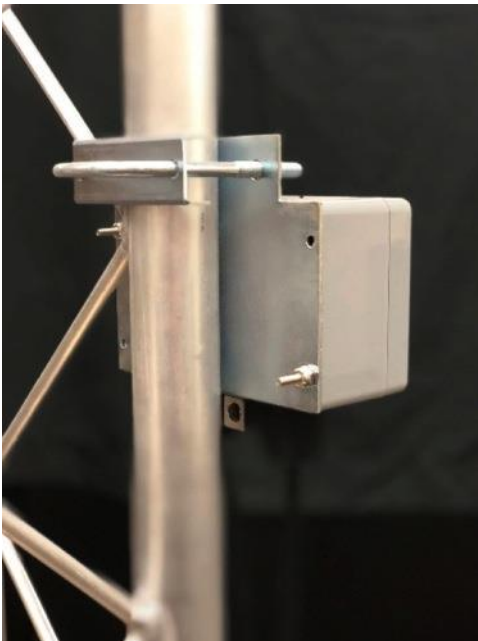


Figure 3. L-Com Lightning Arrestor (Rear View)

Step 2. Connect the Ethernet line cable to the LINE (left) side of the L-Com Lightning Arrestor. It is assumed that the other end of the line cable is plugged in to a POE++ supply.

Step 3. Mount the Pole Mount Bracket Assembly to the pole as shown in Figure 4. Alternatively, discard the back plate for wall mounting options.



Figure 4. Pole Mount Bracket Assembly

Step 4. Mount the V10g Terminal to the Pole Mount Bracket Assembly using the three screws and washers on the back of the terminal (see Figures 5 and 6). The connector ports should face downward.



Figure 5. Mount the V10g Terminal (Front View)

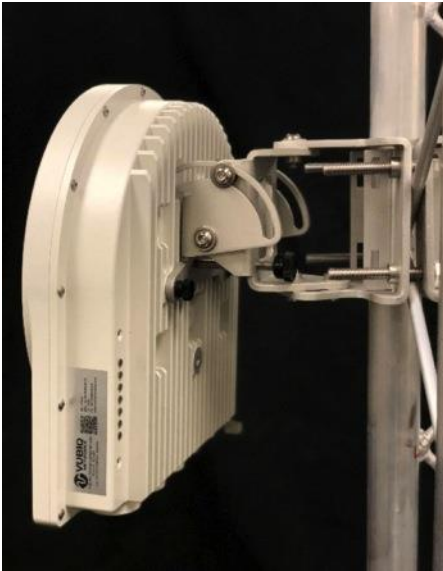


Figure 6. Mount the V10g Terminal (Rear View)

Step 5. Connect earth ground and the ground lug on the terminal to the ground post on the Lightning Arrestor.

Step 6. Connect the 10000Base-X cable to the SFP+ connector to operate at up to 10 Gbps.

Step 7. Connect the 6-foot Ethernet cable between the EQUIP (right) side of the Lightning Arrestor and the first RJ45 port, port P1.

Step 8. During power up, the bottom LED will show dim Green glow.

Step 9. Wait about 45 seconds for the bottom LED to blink Red.

Step 10. Wait about another 10 seconds for the bottom LED to blink Green. The Green blink indicates that the terminal has booted, has started transmitting, and is waiting for a signal to be received from the terminal on the other end of the link. It may take up to 3 minutes before it acquires a signal from the remote unit.

3.4 Alignment

The next steps involve alignment of the V10g. For further details on alignment, please refer to Section 4.0.

Step 11. Attach the Scope Mount and Scope to the terminal (see Figure 7).

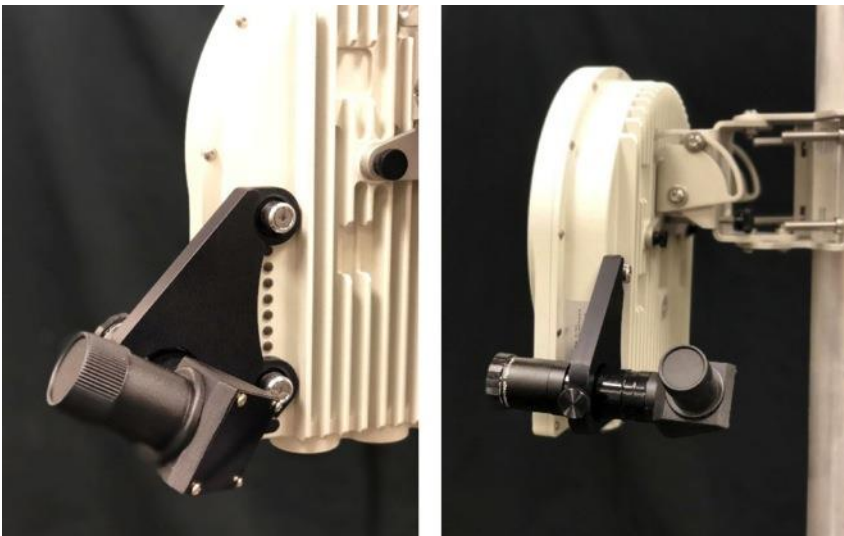


Figure 7. Scope Mount and Scope

Step 12. Optical Adjustment: Align the terminal optically so that the scope cross-hairs are on the terminal on the other side of the link.

Step 13. Coarse Adjustment: Since the terminal is optically aligned, the Bottom LED should change from blinking Green to blinking White, indicating that it is receiving signal from the other end and an RF link has been created. If it is not blinking White, adjust the terminal slightly until it does blink White.

Note: The bottom LED will blink Blue instead of White if the Ethernet mode is set to 2.5 Gbps

The remaining 6 LEDs are used for the fine adjustment. They display two alignment bar graph meters simultaneously.

The Green bar graph meter correlates to signal strength, with more LEDs indicating a stronger signal. The Green LEDs, starting with the bottom one, indicate: > 0 dB, > 10 dB, > 20 dB, > 30 dB, and > 35 dB of attenuation of the incoming signal. The Signal strength in Figure 8 shows that the incoming signal is being attenuated by at least 20 dB.

The Blue bar graph meter indicates signal quality. More LEDs indicate a better RF link. The Blue LEDs, starting with the bottom one, indicate: >= 1.3 Gbps, >= 2.7 Gbps, >= 4.1 Gbps, >= 5.4 Gbps, >= 6.8 Gbps, and >= 8.21 Gbps (Blue) or 10 Gbps (White). A 10 Gbps signal will show 5 Blue LEDs and the top LED will be White as shown in Figure 8.

During the alignment, the 6 LEDs can be Off, Green, Dark Blue, Light Blue (both Green and Blue are on at the same time), or White. Figure 8 shows that the terminal is in 10 Gbps mode (blinking White status LED), the strength of the incoming signal is requiring at least 20 dB of attenuation, and the RF signal is operating at 10 Gbps.

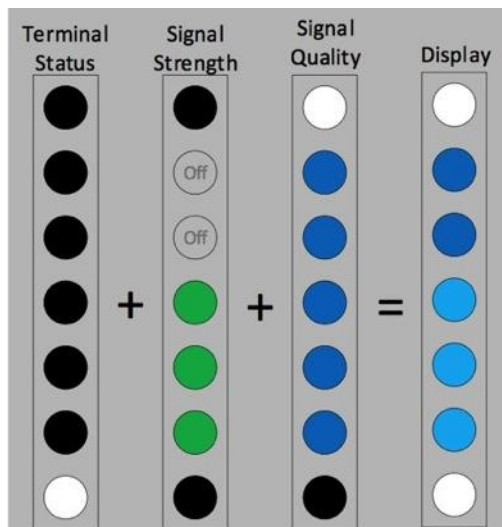


Figure 8. LED Status

Note: During power up and booting, the bottom LED is also used to display Power On Self-Test diagnostic status:

- Dim Green – power is applied. If the LEDs are turned off via the management interface, you will still see the power LED
- Bright Green – POST is running or no signal from the remote terminal
- Bright Red – The RF section is initializing or Error
- Bright Purple – AGC is active

Step 14. Fine Adjustment: Slowly move the terminal in small increments with settling delays between each movement, lighting as many Blue LEDs as possible and turning the top LED White. Maximizing the number of Blue LEDs, dark Blue or light Blue, maximizes the RF signal quality and the RF link data carrying capacity. The Green signal strength is less important than the Blue signal quality.

Step 15. Confirm through a network administrator (or other methods) that data is transmitting across the link.

Step 16. Remove the optical scope and its mounting bracket.

3.5 HaulPass V10g Ports

The HaulPass V10g ports are illustrated in Figure 9.

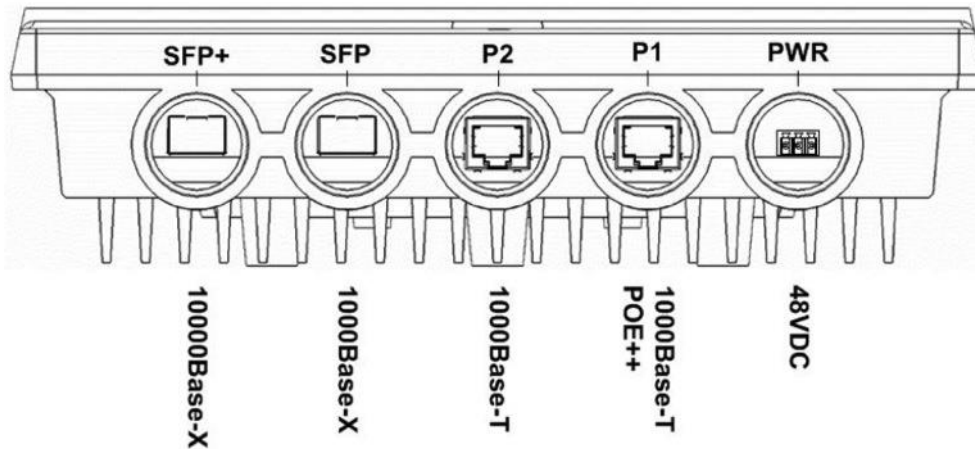


Figure 9. HaulPass V10g Ports

48VDC. This port is used to power up the V10g with an external power supply that is not a POE injector.

1000Base-T / POE++. This port is an RJ45 connector and is Port 1 for the Ethernet switch. It doubles as a power port with a POE++ injector. It is shared with the 1000Base-X port to the internal switch. They cannot both be used for Ethernet at the same time. However, you can power the device with a POE++ through the RJ45 connector and use the 1000Base-X port for Ethernet if there is no Ethernet traffic on the RJ45 port.

1000Base-T. This is an RJ45 connector and is Port 2 for the Ethernet switch.

1000Base-X. This port is an SFP connector and is Port 1 for the Ethernet switch. It is shared with the P1 1000Base-T port to the internal switch. They cannot both be used for Ethernet at the same time. However, you can power the device with a POE++ through the RJ45 connector and use the 1000Base-X port for Ethernet if there is no Ethernet traffic on the RJ45 port.

10000Base-X. This is an SFP+ port that bypasses the switch for communications. Having Ethernet traffic on this port disables the internal switch.

3.6 Power over Ethernet++ Modules

The Vubiq HaulPass V10g ships with a Microsemi 9501GR Power over Ethernet++ (PoE++) injector for powering the Vubiq HaulPass V10g terminal. The power to the V210g terminal travels over a CAT5E / CAT6 cable that is plugged into terminal P1, 1000Base-T. The PoE++ module accepts AC Power from 100 to 240 VAC at 50 or 60 Hz. The port labeled DATA PWR OUT (closest to the power LED) should be connected to the V10g. The port labeled DATA IN should be connected to your network.

The user may use a different PoE device such as a network switch provided the device is PoE++ and can supply 45 watts of power at 48 volts.

If the user would like to power the terminal with DC Power the 48VDC port should be used.

It is possible to have redundant power supplies by using both PoE++ and the 48 VDC ports simultaneously.

3.7 Lightning/Surge Protection



Vubiq Networks, Inc. strongly suggests that installer use a surge suppressing lightning arrestor on any copper cable that will be connected to the HaulPass V10g. An L-Com Lightning Arrestor is shipped with the terminal for this purpose and will provide protection for the PoE++ P1 port. If the user chooses to use the 48VDC power port, the P2 port, or copper on the 1000Base-X or 10000Base-X ports additional lightning arrestors should be installed for those ports.

3.8 Grounding



A ground wire must be connected between the ground lug and the metal mounting mast. Verify that the metal mast is electrically connected to the structure ground. Improper structure-to-earth grounding can result in electromagnetic interference and susceptibility to electrical discharge. Incorrect grounding will void the warranty of the HaulPass V10g. In addition, Vubiq strongly recommends the use of outdoor surge/lightning protectors.

4.0 Alignment Details

For basic alignment procedures, please refer to Section 3.4. Provided below are additional alignment details.

4.1 HaulPass V10g Throughput

Figure 10 is a graph illustrating HaulPass V10g throughput. It shows what to expect in the way of throughput, modulation and profile.

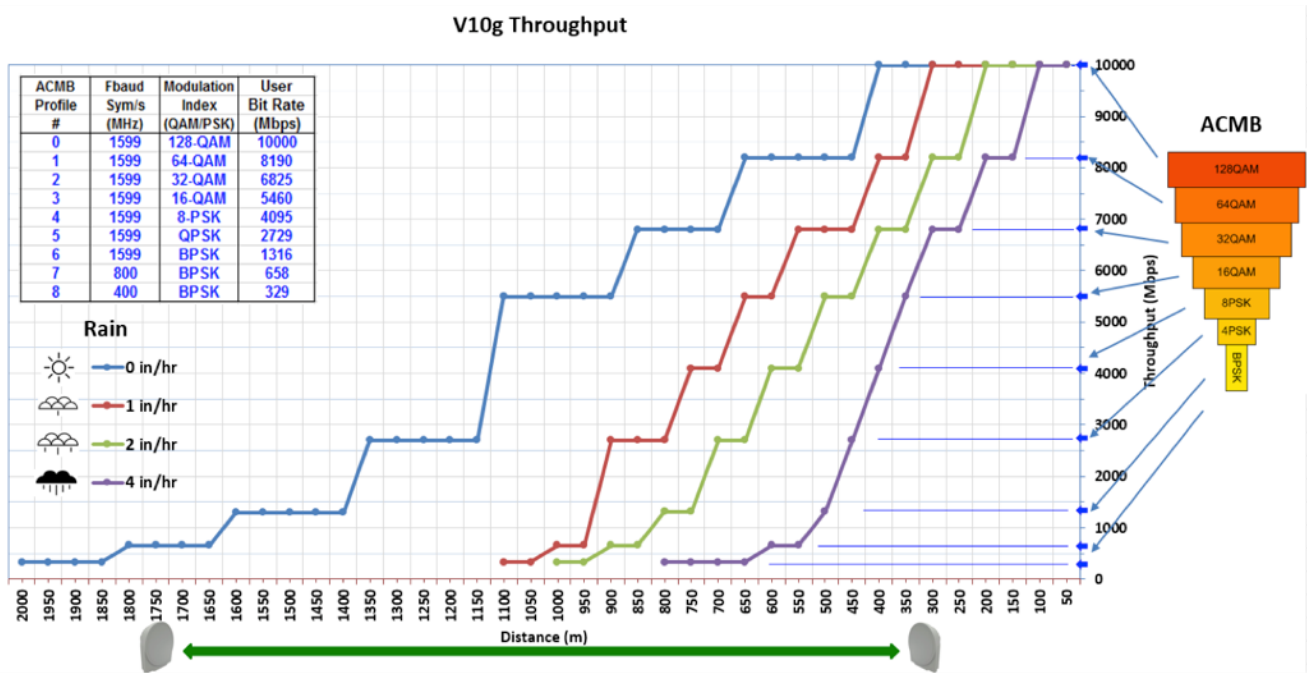


Figure 10. HaulPass V10g Throughput, Modulation and Profile Graph

4.2 Alignment Procedure

To align the V10g, first align optically via the scope as described in Section 3.4. This is the course alignment.

The next step is LED alignment. This is the fine adjustment. Most customers will not need to do anything past optical alignment and checking the LEDs. Table 2 shows the expected throughput and expected LEDs.

Table 2. V10g Expected Throughput and Expected LEDs

Profile	Modulation (QAM/PSK)	MBaud	User Bit Rate (Gbps)	Minimum Normalized MSE (SNR)	LEDs to expect (Heartbeat will be White in 10G mode and Blue in 2.5G mode)
0	128-QAM	1599	10.0	-24.6	All remaining LEDs will be blue with the last one being white
1	64-QAM	1599	8.2	-21.8	All remaining LEDs will be blue
2	32-QAM	1599	6.8	-18.8	Five LEDs will be blue
3	16-QAM	1599	5.4	-15.8	Four LEDs will be blue
4	8-PSK	1599	4.1	-12.8	Three LEDs will be blue
5	QPSK	1599	2.7	-10.8	Two LEDs will be blue
6	BPSK	1599	1.3	-7.8	One LED will be blue
7	BPSK	800	0.6	-4.8	No other LEDs will be blue
8	BPSK	400	0.3	-3.0	No other LEDs will be blue

The heartbeat LED will be White in 10G mode or Blue in 2.5G mode (LED closest to the ports).

- This means you have RF end to end connectivity.
- Prior to RF connectivity this LED will blink green
- When connectivity starts this LED will go purple for a brief period during the initial AGC time.

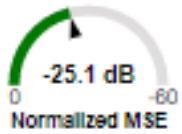
Fine adjust to get the most blue (light or dark blue) LEDs.

- The more blue LEDs the more throughput.
- If the LED furthest from the ports (furthest from the heartbeat LED) is white you have 10G end to end connectivity. (See table)
- The lighter color blue is actually a combination of blue and green LEDs. If you have many light blue LEDs that means you have a lot of attenuation which means you have some additional margin vs. rain and/or your link is short. Longer links will have less light blue at the same throughput.

4.3 Mean Squared Error (MSE)

Mean Squared Error (SNR with the opposite sign) can be used for ultra fine adjustment. This adjustment is only needed to squeeze out a little extra margin. If the optical alignment is good and the LEDs are as expected, this may be unnecessary.

Maximize the magnitude of the MSE (see the web interface). The larger the number, the better.



MSE can be used to calculate Signal to Noise Ratio (SNR) with just a change in the sign of the number. For example, -25.1 dB MSE = 25.1 dB SNR.

Note: MSE is used to determine which ACMB profile is selected. See Table 2.

Note: SNR or MSE always correlates to the signal quality and quality of alignment and minimum Bit Error Rate (BER).

5.0 Additional Instructions

5.1 Changing from 10 Gbps/10000Base to 2.5 Gbps/1000Base

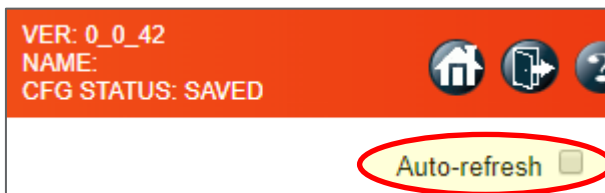
In 10 Gbps/10000Base mode, the default mode from the factory, only the data presented on the SFP+ port is transmitted to the remote terminal and the data from the remote terminal is only presented to the SFP+ port. If you want the RF signal to carry data from the 1000Base ports, you will need to put the link in to the 2.5 Mode instead of the 10.0 Mode.

Note: Both terminals in a link must be operating in the same RF Mode in order to establish a link. Change the RF Mode on the far side terminal before changing the RF Mode on the near side terminal as the communication link will not function while the two terminals are in different RF Modes.

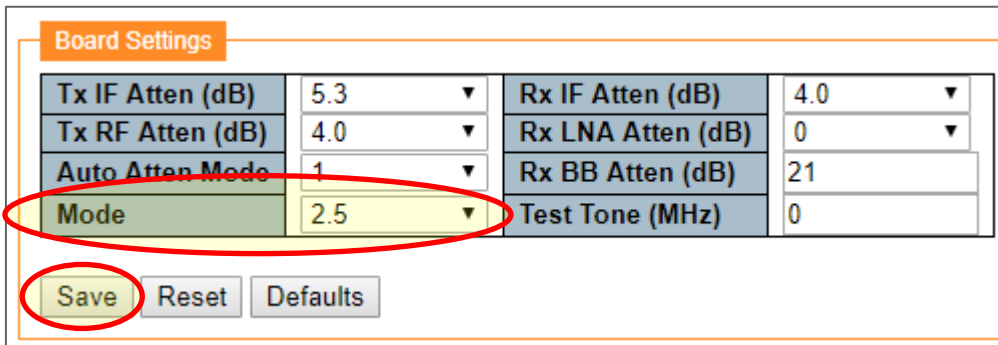
Note: The terminals ship in 10.0 RF Mode. Unless a connection is made on the remote terminal between the Base1000 port and the Base10000 network, you will not be able to reach the management unit on the far side.

Changing the Mode via the Webpage

Log in to the terminal with an account that has administrative privileges. On the main RF page, clear the Auto-refresh check box in the upper right corner of the webpage.



Under Board Settings, choose the Mode drop down and select the desired mode and then press the Save button. The Auto-refresh will be automatically re-enabled. There is no need for an additional save.



Changing the Mode via the CLI

The command to verify the current RF Mode via the CLI is `rf mode`.

```
# rf mode
10.0
# rf mode 2.5
# rf mode
2.5
# rf mode 10.0
# rf mode
10.0
#
```

5.2 Changing the IPv4 Address

Changing the Address via the Webpage

Log in to the terminal with an account that has administrative privileges. On the menu on the left side of the screen select Configuration → System → IP.

V10g™ Vubiq Networks Radio

IP Configuration

Mode: Host

DNS Server 0: No DNS server

DNS Server 1: No DNS server

DNS Server 2: No DNS server

DNS Server 3: No DNS server

DNS Proxy:

IP Interfaces

Delete	VLAN	DHCPv4			IPv4	
		Enable	Fallback	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.66.2	24

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save (circled) Reset

In the IPv4 field enter the new address and then press the Save button. The terminal's IPv4 address will change immediately when the Save button is pressed and you will lose your webpage connection to the terminal. Change your browser's destination to the new IPv4 address and log in again using an account that has administrative privileges.

After logging in the configuration must be saved as the Startup-Configuration to retain the new IPv4 address through a reboot or power cycle. You will be able to confirm that the startup-config needs to be saved by way of an informational message in the upper right corner of the webpage.

VER: 0_0_42
NAME
CFG STATUS: SAVE startup-config

On the left side menu choose Maintenance → Configuration → Save startup-configuration.

VUBIQ NETWORKS V10

Configuration

Monitor

System

Thermal Protection

Ports

State

Traffic Overview

QoS Statistics

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be ti

Save Configuration (circled)

Press the Save Configuration button. You will receive a confirmation that the startup-config was saved successfully.

Changing the Address via the CLI

Use telnet to log in to the terminal with an account that has administrative privileges.

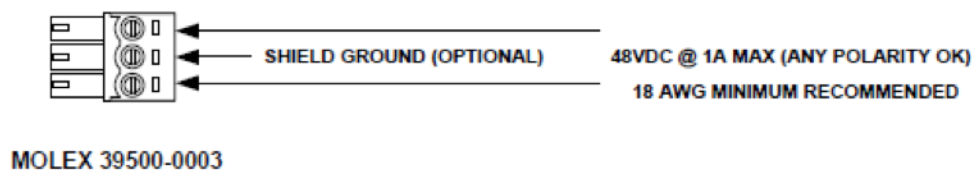
```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.66.4 255.255.255.0
(config-if-vlan)#
```

At this point you will lose your connection to the terminal and must log in again at the new IPv4 address to save the running-config to the startup-config.

```
# copy running-config startup-config
Building configuration...
% Saving 1392 bytes to flash:startup-config
#
```

5.3 Using the 48VDC Power Port

Connect the supplied 48VDC connector as shown in Figure 11 below.



Example Cable Recommendations

- Belden 5340F1 Shielded 2-conductor 18 AWG outdoor
- Belden 5240F1 Shielded 2-conductor 16 AWG outdoor
- Belden 1307A Unshielded 2-conductor 16 AWG outdoor

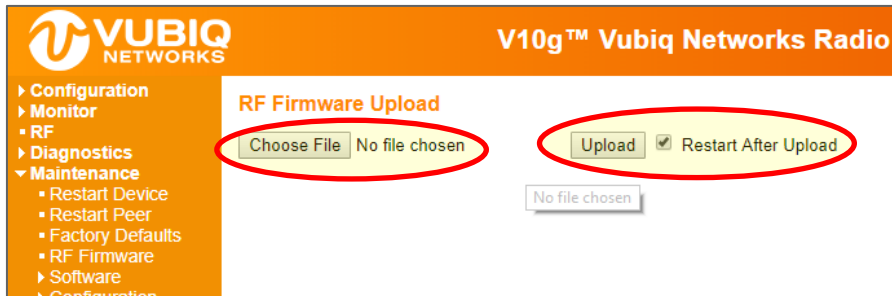
Figure 11. Connecting the 48VDC Power Port

5.4 Upgrading the Firmware

The internal design of the V10g consists of 2 separate processors that make up the system: the RF processor and the network switch processor. Each processor runs its own firmware image, and these firmware images are updated independently when necessary. During a firmware update process, the V10g system will continue to function, running the currently loaded firmware. Once the firmware update process completes, the V10g system will reboot itself and load the upgraded firmware image. It is only during the system reboot portion of the firmware upgrade process that the V10g communication is temporarily interrupted.

Upgrading the RF Firmware

The RF processor firmware can be upgraded by selecting the Maintenance > RF Firmware menu item from the web GUI:



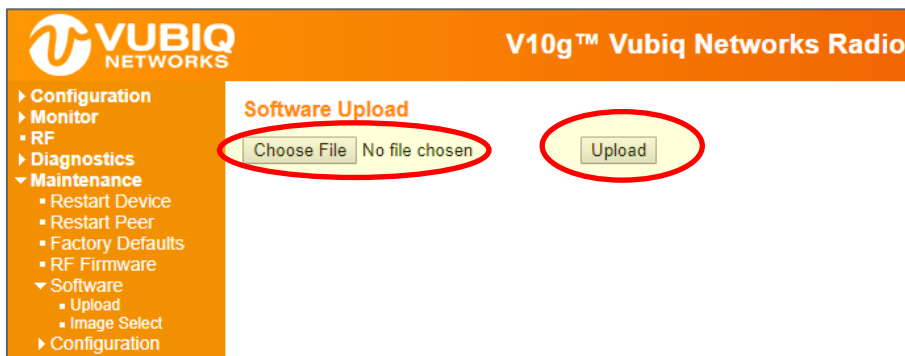
First press the Choose File button to browse to the location of an RF firmware image. Then press the Upload button to start the upgrade process. After the RF firmware image is uploaded, a web page announces that the firmware update is initiated. After the upload completes and is transferred to the RF system, the firmware is updated and the system will restart automatically.



Warning: Do not restart or power off the device during the firmware upgrade process. Doing so may cause the RF processor to fail to function as a result.

Upgrading the Network Switch Firmware

The network switch firmware can be upgraded using by selecting the Maintenance > Software > Upload menu item from the web GUI:



First press the Choose File button to browse to the location of the desired network switch firmware image. Then press the Upload button to start the upgrade process. After the network switch firmware image is uploaded, a web page announces that the firmware update is initiated. After the upload completes and is transferred to the network switch, the firmware is updated and the system will restart automatically.



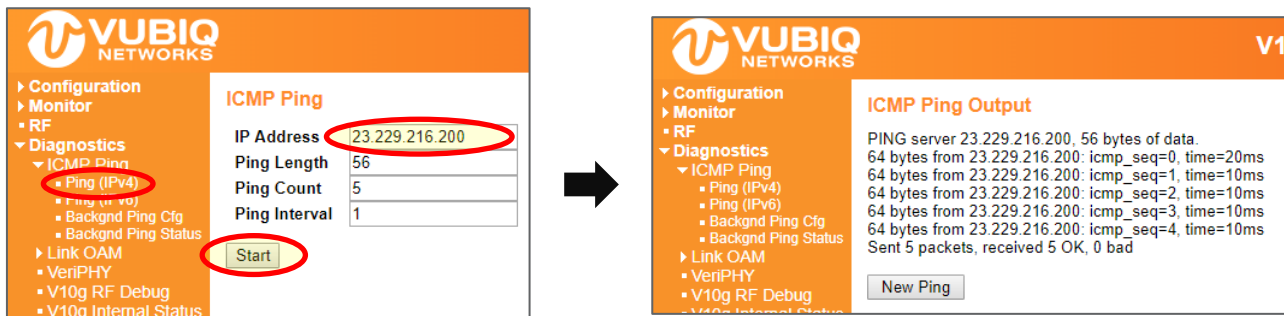
Warning: Do not restart or power off the device during the firmware upgrade process. Doing so may cause the network switch to fail to function as a result.

5.5 Changing the Clock Time

The HaulPass V10g terminal boots with the standard UNIX Epoch time of midnight January 1, 1970 UTC and counts up from there. This is the time that is used for the internal logs. This time is sufficient for many installations, but there are situations that require the use of the current time. Using the current time can make reviewing the internal logs easier to correlate with real world events. This section describes how to use a time server to change the HaulPass V10g to the current time.

Configuring the Network

The first step is to configure your network so that the HaulPass V10g can communicate with a time server. If you cannot reach the Internet from the HaulPass V10g, you will not be able to reach a timer server. Once you have configured your network so that the HaulPass V10g can reach the Internet, you are ready to test the connection with a ping. Most time servers do not support ping, so you will need to ping another host on the Internet. The vubiqnetworks.com server is at 23.229.216.200. You can ping the vubiqnetworks.com server from both the Web GUI and the command line.

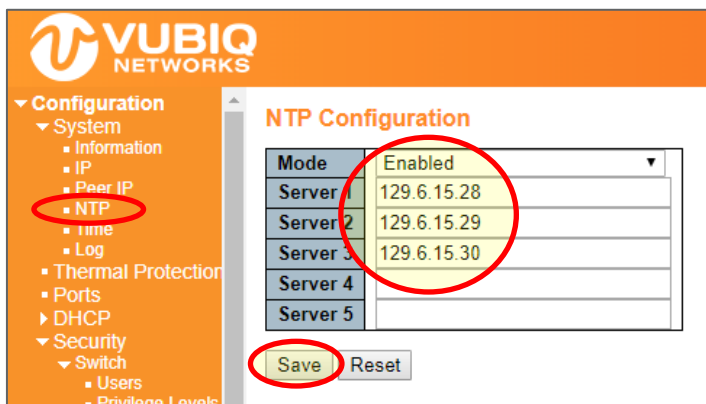


```
# ping ip 23.229.216.200
```

```
PING server 23.229.216.200, 56 bytes of data.
64 bytes from 23.229.216.200: icmp_seq=0, time=20ms
64 bytes from 23.229.216.200: icmp_seq=1, time=10ms
64 bytes from 23.229.216.200: icmp_seq=2, time=10ms
64 bytes from 23.229.216.200: icmp_seq=3, time=10ms
64 bytes from 23.229.216.200: icmp_seq=4, time=10ms
Sent 5 packets, received 5 OK, 0 bad
#
```

Pointing to the NIST Internet Time Servers

We recommend using the [NIST Internet Time Servers](#) for your clock time reference. The first three IP addresses on their list are 129.6.15.28, 129.6.15.29, and 129.6.15.30, so these are the three used in this example.



```

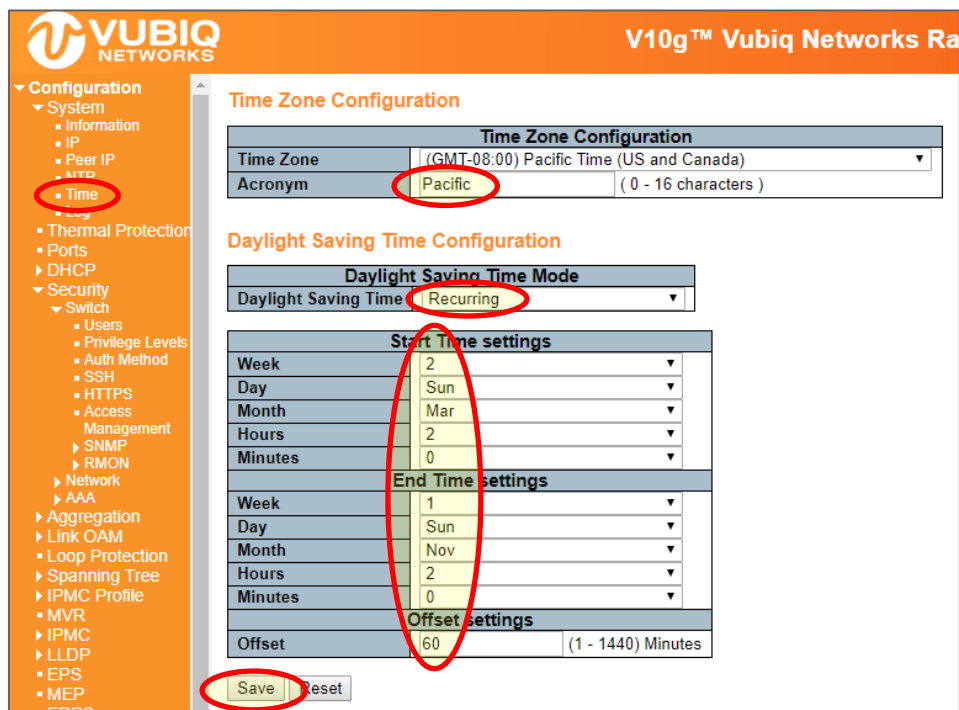
# show ntp status
NTP Mode : disabled
Idx   Server IP host address (a.b.c.d) or a host name string
----  -----
1
2
3
4
5
# configure terminal
(config)# ntp server 1 ip 129.6.15.28
(config)# ntp server 2 ip 129.6.15.29
(config)# ntp server 3 ip 129.6.15.30
(config)# ntp
(config)# exit
# show ntp status
NTP Mode : enabled
Idx   Server IP host address (a.b.c.d) or a host name string
----  -----
1     129.6.15.28
2     129.6.15.29
3     129.6.15.30
4
5
#

```

Configuring the Local Time Zone

Now that the HaulPass V10g can reach the NIST Internet Time Servers, it is able to obtain the UTC time. However, UTC is probably not your local time zone, so you need to configure the offset from UTC and to program Daylight Saving Time as applicable. The example below shows a terminal in California, which is Pacific Time with Daylight Saving Time.

Most of the United States begins Daylight Saving Time at 2:00 a.m. on the second Sunday in March and reverts to standard time on the first Sunday in November. Some time zones switch at a different time.



VUBIQ NETWORKS V10g™ Vubiq Networks Ra

Configuration

- System
 - Information
 - IP
 - Peer IP
 - MTD
 - Time**
 - Log
- Thermal Protection
- Ports
- DHCP
- Security
 - Switch
 - Users
 - Privilege Levels
 - Auth Method
 - SSH
 - HTTPS
 - Access Management
 - SNMP
 - RMON
 - Network
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - EPS
 - MEP
 - EDPS

Time Zone Configuration

Time Zone Configuration	
Time Zone	(GMT-08:00) Pacific Time (US and Canada)
Acronym	Pacific (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode

Daylight Saving Time: Recurring

Start Time settings

Week	2
Day	Sun
Month	Mar
Hours	2
Minutes	0

End Time settings

Week	1
Day	Sun
Month	Nov
Hours	2
Minutes	0

Offset settings

Offset	60 (1 - 1440) Minutes
--------	-----------------------

Save Reset

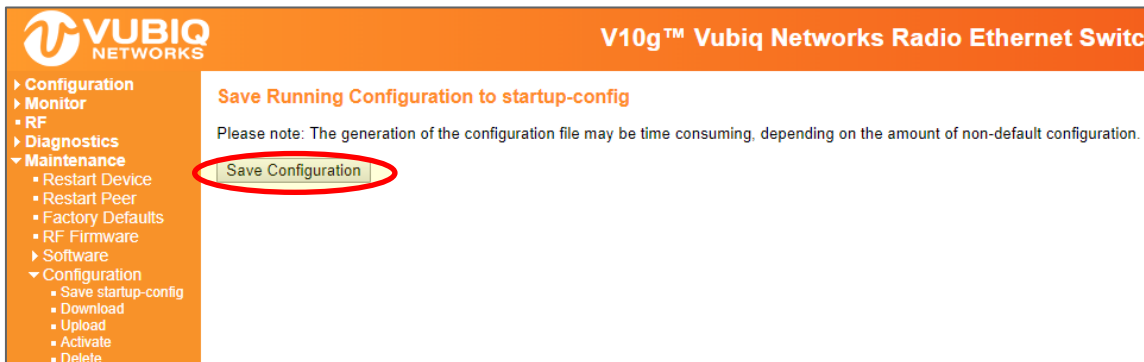
```
# configure terminal
(config)# clock timezone Pacific -8
(config)# clock summer-time PDT recurring 2 7 3 02:00 1 7 11 02:00
(config)# exit
# show clock detail
System Time      : 2017-02-03T13:26:36-08:00

Timezone : Timezone Offset : -4800 ( -480 minutes)
Timezone Acronym : Pacific

Daylight Saving Time Mode : Recurring.
Daylight Saving Time Start Time Settings :
    * Week: 2
    * Day: 7
    * Month: 3
      Date: 0
      Year: 0
    * Hour: 2
    * Minute: 0
Daylight Saving Time End Time Settings :
    * Week: 1
    * Day: 7
    * Month: 11
      Date: 0
      Year: 0
    * Hour: 2
    * Minute: 0
Daylight Saving Time Offset : 1 (minutes)
#
```

Saving the Configuration

At this point, if you are satisfied with the settings for using the NIST Internet Time Server and the offset from UTC, you will need to save the configuration to the startup-configuration. If you don't save it to the startup-configuration, then the configuration will be lost with the next reset or power cycle.



The screenshot shows the Vubiq V10g web interface. The top header is orange with the Vubiq Networks logo on the left and the text "V10g™ Vubiq Networks Radio Ethernet Switch" on the right. A left-hand navigation menu is visible, listing categories like Configuration, Monitor, RF, Diagnostics, Maintenance, Software, and Configuration. The "Save Configuration" button in the Maintenance section is circled in red. The main content area displays the heading "Save Running Configuration to startup-config" and a note: "Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration."

5.6 Setting https Web Access

This section describes how to set up https web access for the HaulPass V10g. If you need a certification certificate, you will need to obtain it from one of the many official certificate authorities. Alternatively, if the V10g is only being used within your own network, then you may generate your own certification, known as a self-certified certificate.

The HaulPass V10g provides two options for self-certification: a built-in certificate generator for minimal security, or the option to generate a more secure key as described below.

Step 1: First you will need OpenSSL. This is included on most Linux distributions. Binaries are available at <https://slproweb.com/products/Win32OpenSSL.html> and elsewhere.

Step 2: Then you will need to create a certificate and key. This example generates a 2048 bit sha256 key. From a Windows or Linux command line, type the following in bold:

```
C:\OpenSSL-Win64\bin>openssl req -x509 -sha256 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365
```

The following will be displayed on your screen:

```
Generating a 2048 bit RSA private key
```

```
.....
```

```
.....+++
```

```
.....+++
```

```
writing new private key to 'key.pem'
```

```
Enter PEM pass phrase:
```

```
Verifying - Enter PEM pass phrase:
```

```
-----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [AU]:US
```

```
State or Province Name (full name) [Some-State]:CA
```

```
Locality Name (e.g., city) []:Irvine
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Vubiq
```

```
Organizational Unit Name (eg, section) []:
```

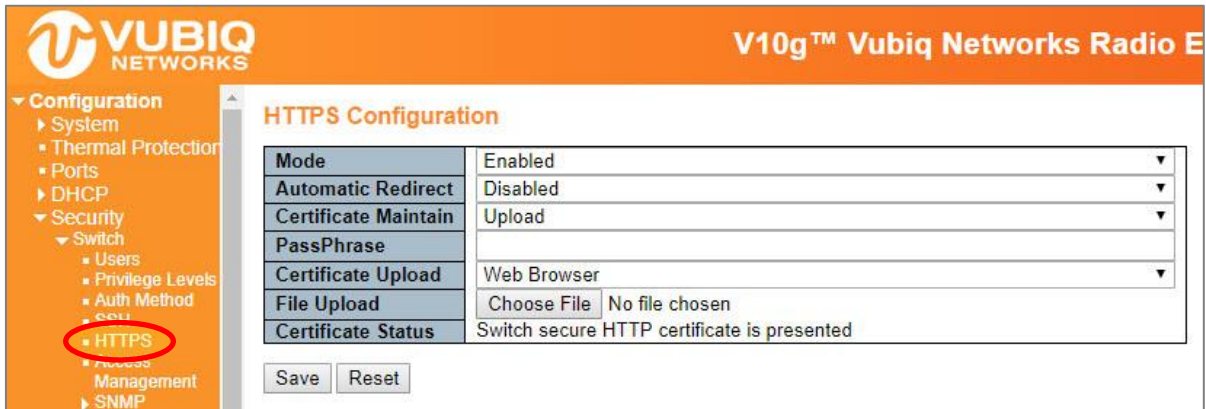
```
Common Name (e.g. server FQDN or YOUR name) []:
```

```
Email Address []:
```

Step 3: Now you will need to combine the certificate and key. From the same command line as above, type the following in **bold** onto the command line:

```
C:\OpenSSL-Win64\bin>copy cert.pem+key.pem cert_key.pem
cert.pem
key.pem
1 file(s) copied.
C:\OpenSSL-Win64\bin>
```

Step 4: Now upload your combined certificate and key file in the https page. Remember to type in the passphrase that you entered when you generated the key and certificate.



VUBIQ NETWORKS V10g™ Vubiq Networks Radio E

Configuration

- System
- Thermal Protection
- Ports
- DHCP
- Security
 - Switch
 - Users
 - Privilege Levels
 - Auth Method
 - SSH
 - HTTPS**
 - Access Management
 - SNMP

HTTPS Configuration

Mode	Enabled
Automatic Redirect	Disabled
Certificate Maintain	Upload
PassPhrase	
Certificate Upload	Web Browser
File Upload	Choose File No file chosen
Certificate Status	Switch secure HTTP certificate is presented

Save Reset

Note: Chrome and other browsers will warn you that the site is self-certified. However, this procedure will allow secure access to your HaulPass V10g.

5.7 Restoring to Factory Default IP Address and Password

This section describes how to restore your HaulPass V10g to the factory default IP address and password. Two alternative methods are available: manual process and GUI process.

Manual Process

This process is most easily accomplished at a desk, but can also be completed at the installed location.



Note: Restoring factory defaults will set all user accounts back to the factory settings. Any stored passwords and/or accounts will be reset.

First, connect the “POE Injector Out” to Port 1 of the V10g (black cable in photo below) and connect the “POE Injector In” to Port 2 of the V10g. This creates a loopback through the POE. Note that this procedure cannot be completed through a switch. Once configured as shown in Figure 12, power cycle the V10g by power cycling the POE injector.

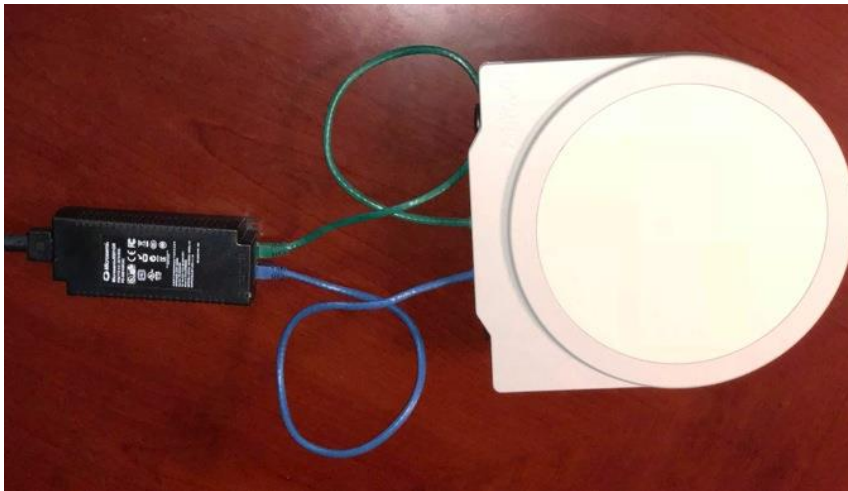
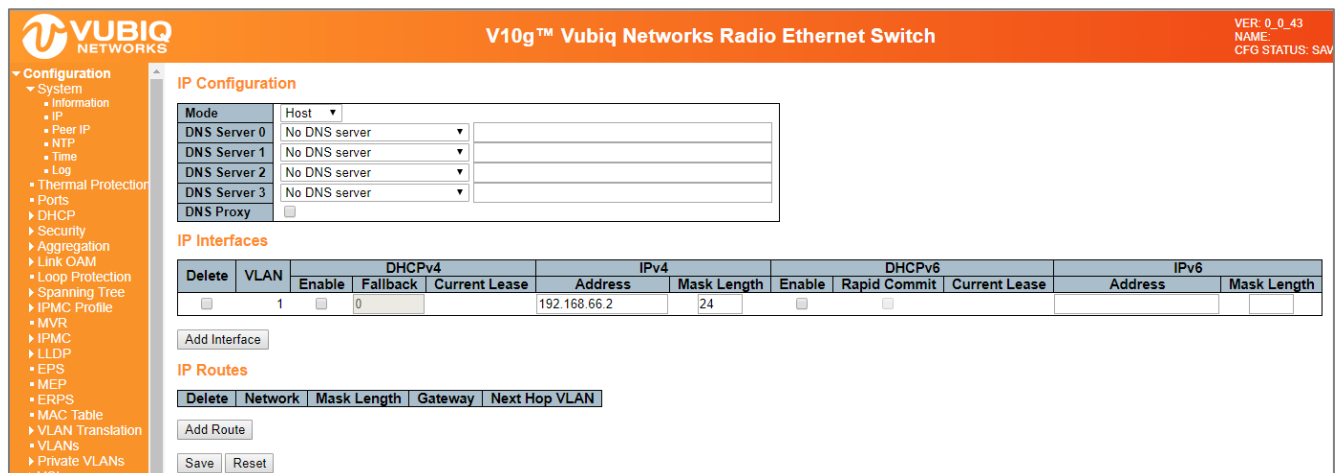


Figure 12. Restoring the V10g to Factory Default IP Address and Password

Wait a full three minutes. Then, without powering down, take the blue cable (the cable that was feeding Port 2) and connect it directly to a PC. At this point the IP address will be 192.168.66.2.

The login will now be “admin” with no password. You can now change the IP address and other network settings. Once complete, save your settings twice when on the relevant page and also in Maintenance > Configuration > Save startup-config. Note that once you change the IP address, you will need to login again with the new IP address before you can save the configuration. During this time, do not shut off power.



Vubiq Networks V10g™ Vubiq Networks Radio Ethernet Switch

VER: 0_0_43
NAME:
CFG STATUS: SAV

IP Configuration

Mode	Host
DNS Server 0	No DNS server
DNS Server 1	No DNS server
DNS Server 2	No DNS server
DNS Server 3	No DNS server
DNS Proxy	<input type="checkbox"/>

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.66.2	24	<input type="checkbox"/>	<input type="checkbox"/>			

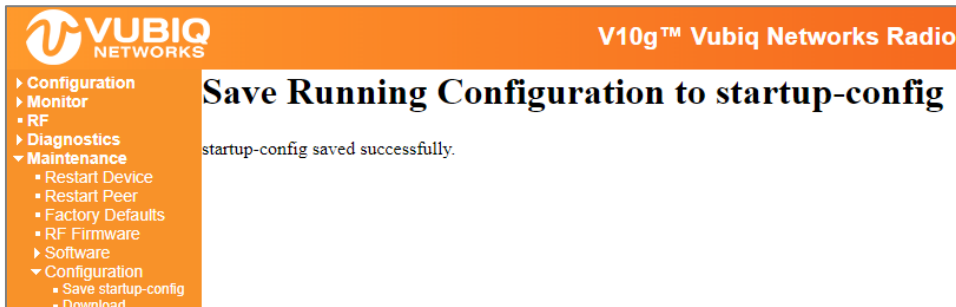
Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save Reset

GUI Process

if login is possible, an alternative approach to resetting to factory defaults is to use the Maintenance > Factory Defaults menu option.



Note: Restoring factory defaults will set all user accounts back to the factory settings. Any stored passwords and/or accounts will be reset.

Choosing this command option and then selecting the Yes button will reset the configuration to Factory Defaults. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart and no “second save” of the configuration is necessary.

Note: If you select the No button on the page, you will return to the main RF page without resetting the configuration.

From the command line:

Attempt to keep VLAN1 IP setup

```
# reload defaults keep-ip
```

```
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
```

```
#
```

Or resetting the IP Address back to 192.168.66.2

```
# reload defaults
```

```
% Reloading defaults. Please stand by.
```

```
#
```


6.0 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.

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

Web GUI Example: Change the aging time to 600 seconds:



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time seconds

MAC Table Learning

	Port Members			
	1	2	3	4
Auto	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members			
			1	2	3	4

Add New Static Entry

Save Reset

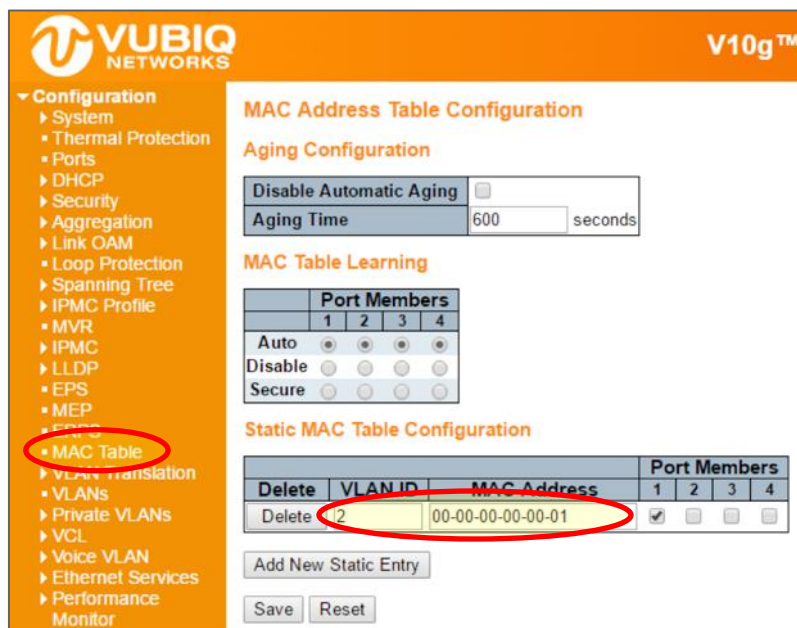
Figure 13. Change the Aging Time to 600 Seconds

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

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



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time seconds

MAC Table Learning

	1	2	3	4
Auto	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members			
			1	2	3	4
Delete	2	00-00-00-00-00-01	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Static Entry

Save Reset

Figure 14. Static MAC Address Configuration

6.3 Showing the MAC Address Table

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

```
# show mac address-table
Type    VID  MAC Address          Ports
Static  1    33:33:00:00:00:01   GigabitEthernet 1/1-4 CPU
Static  1    33:33:00:00:00:02   GigabitEthernet 1/1-4 CPU
Static  1    33:33:ff:00:0c:81   GigabitEthernet 1/1-4 CPU
Static  1    68:28:f6:00:0c:81   CPU
Dynamic 1    8c:ae:4c:f4:01:03   GigabitEthernet 1/2
Static  1    ff:ff:ff:ff:ff:ff   GigabitEthernet 1/1-4 CPU
Static  2    00:00:00:00:00:01   GigabitEthernet 1/1
#
```

The current MAC address table can be viewed with the WEB GUI as well:

VUBIQ NETWORKS V10g™ Vubiq Networks Rack

Configuration
 Monitor
 System
 Thermal Protection
 Ports
 State
 Traffic Overview
 CoS Statistics
 QCL Status
 Detailed Statistics
 Link OAM
 DHCP
 Security
 LACP
 Loop Protection
 Spanning Tree
 MVR
 IPMC
 LLDP
 Ethernet Services
 Performance
MAC Table

MAC Address Table

Start from VLAN and MAC address with entries per page.

Type	VLAN	MAC Address	Port Members			
			CPU 1	2	3	4
Static	1	33-33-00-00-00-01	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓
Static	1	33-33-FF-01-D4-CE	✓	✓	✓	✓
Static	1	68-28-F6-01-D4-CE	✓			
Dynamic	1	8C-AE-4C-F4-1E-EC	✓			
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓
Static	12	00-00-00-00-00-01	✓			

Figure 15. MAC Address Table

7.0 VLAN

7.1 VLAN Quick Configuration Example

V10g™ Vubiq Networks Radio Ethernet Switch

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 16. Default VLAN Configuration

Because VLAN 1 is created by default, we need only add VLAN 2 as follows:

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

V10g™ Vubiq Networks Radio Ethernet Switch

Global VLAN Configuration

Allowed Access VLANs	1,2
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

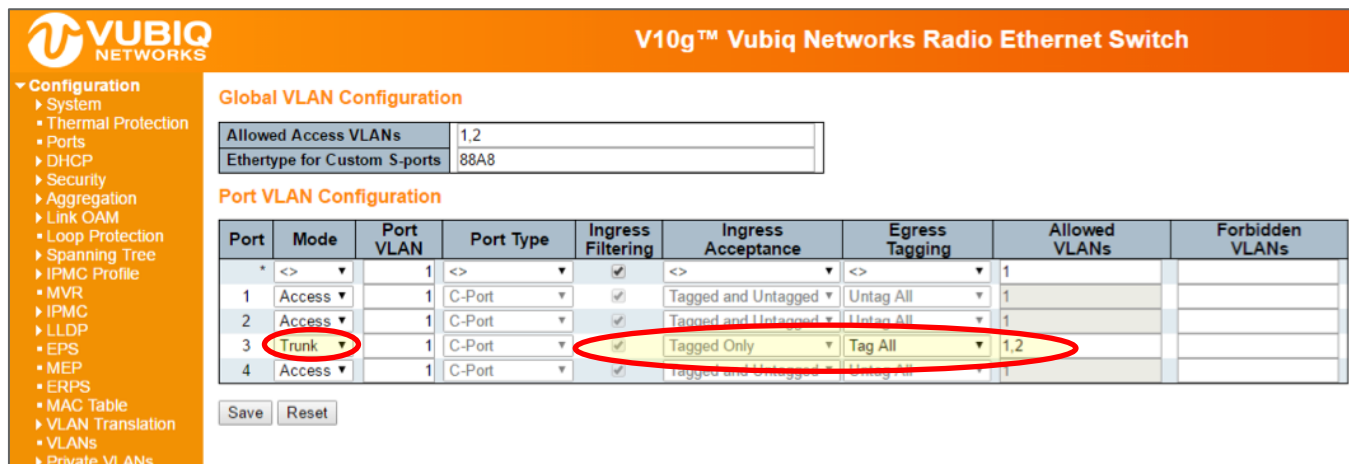
Figure 17. Creating VLAN 2

Set the access port. Assume that ports 1 and 2 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-if)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# exit
(config)# exit
#
```

Set the trunk port. Port 3 is the radio connection to the other Vubiq HaulPass V10g. Set the allowed VLAN to accept 1 & 2.

```
# configure terminal
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-2
(config-if)# switchport trunk vlan tag native
(config-if)# exit
(config)# exit
#
```



VUBIQ NETWORKS V10g™ Vubiq Networks Radio Ethernet Switch

Global VLAN Configuration

Allowed Access VLANs: 1,2
 Ethertype for Custom S-ports: 88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,2	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 18. Setting the Trunk Port

7.2 Global Configuration

Existing VLAN

CLI example – adding VLAN 2:

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

CLI example – removing VLAN 2:

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

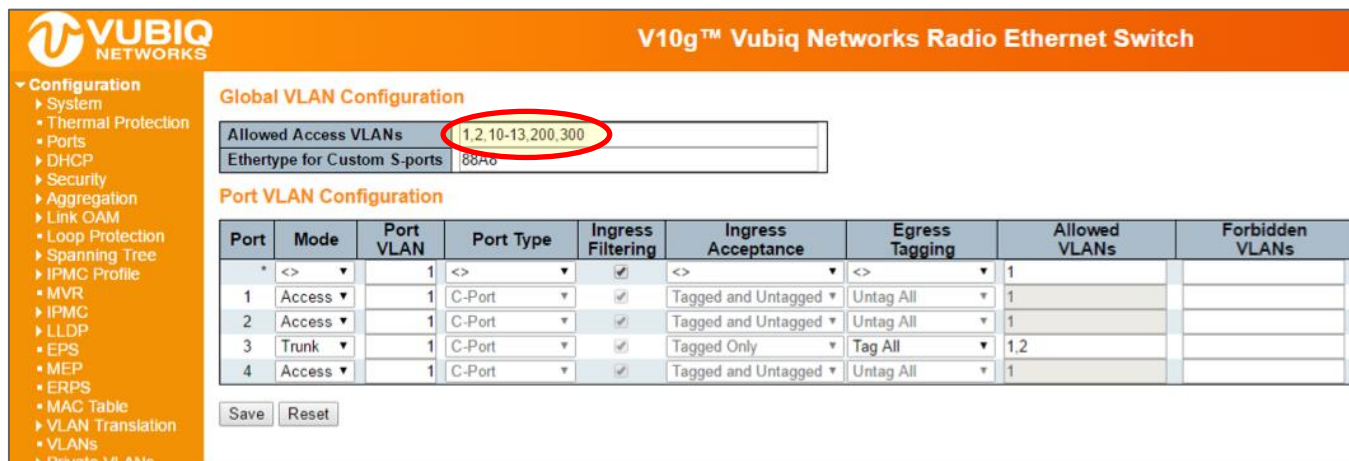
CLI example – show existing VLANs:

```
# show vlan brief
VLAN Name
-----
1 default Gi 1/1-4
2 VLAN0002 Gi 1/3
#
```

The Allowed Access VLAN field only affects ports configured as access ports. Ports in other modes are members of all VLANs specified in the allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using the following list syntax:

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

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 example creates VLANs 1, 10, 11, 12, 13, 200, and 300.



Global VLAN Configuration

Allowed Access VLANs: 1,2,10-13,200,300

Ethertype for Custom S-ports: 88A6

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,2	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 19. VLAN Allowed Access VLANs Configuration

VLAN Naming

CLI example – set VLAN 2's name to test:

```
# configure terminal
(config)# vlan 2
(config-vlan)# name test
(config-vlan)# exit
(config)# exit
# show vlan brief
VLAN  Name                               Interfaces
-----
1      default                                Gi 1/1-4
2      test                                   Gi 1/3
10     VLAN0010
11     VLAN0011
12     VLAN0012
13     VLAN0013
200    VLAN0200
300    VLAN0300
#
```

Web GUI not available.

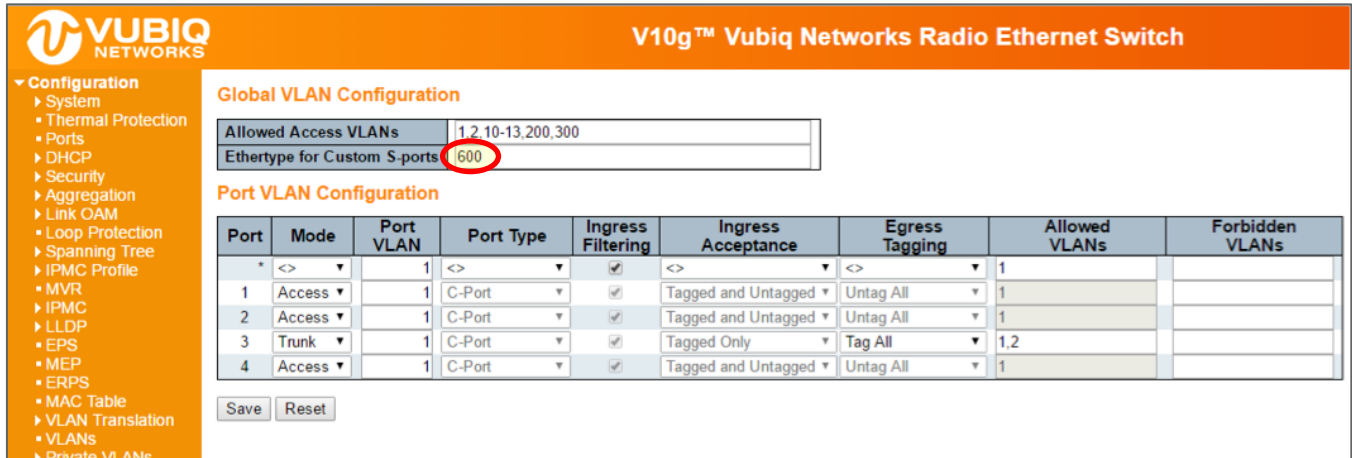
Ethertype for Custom S-ports

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. The example below is setting the EtherType to 0x600 but any value in the range of <0x0600 – 0xffff> is allowed.

CLI example:

```
# configure terminal
(config)# vlan ethernet s-custom-port 0x600
(config)# exit
#
```

Web GUI Example:



Global VLAN Configuration

Allowed Access VLANs: 1,2,10-13,200,300

Ethertype for Custom S-ports: 600

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,2	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 20. VLAN Ethertype for Custom S-ports Configuration

7.3 Port-based Configuration

Port Mode

Port mode determines the fundamental behavior of the port in question. A port can be in one of three modes, 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 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:

Member of all existing VLANs by default (limited by the use of allowed VLANs).

All frames except those classified to the Port VLAN or Native VLAN get tagged on egress by default (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 the following 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:

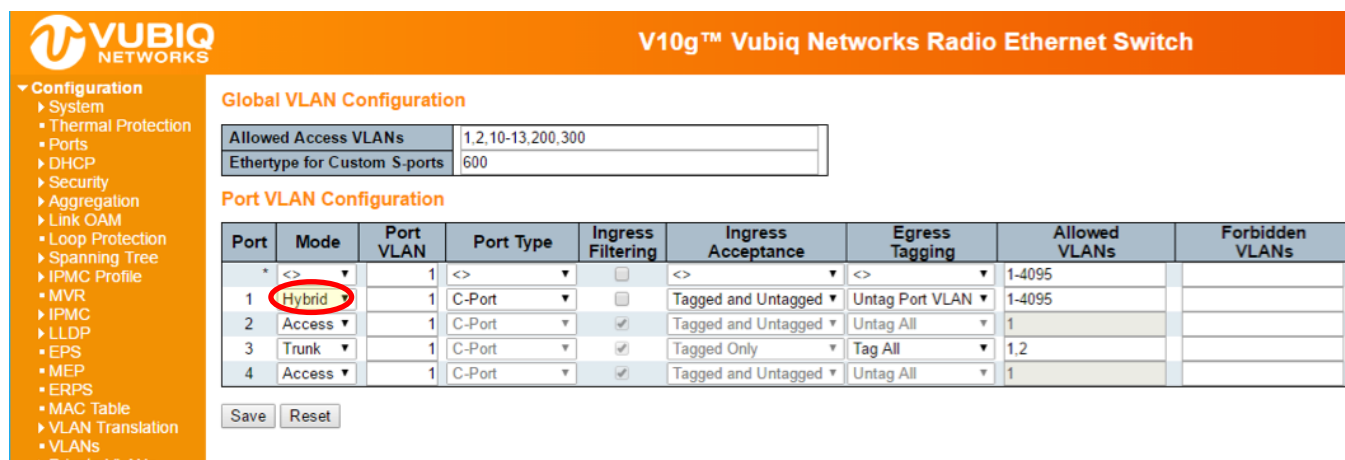
```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# exit
(config)# exit
#
```

CLI example – configure as Trunk port on the first Gigabit port:

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

CLI example – configure as Hybrid port on the first Gigabit port:

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



V10g™ Vubiq Networks Radio Ethernet Switch

Global VLAN Configuration

Allowed Access VLANs	1,2,10-13,200,300
Ethertype for Custom S-ports	600

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Hybrid	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,2	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 21. VLAN Mode Configuration

Port VLAN

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.

On 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 is set to untag port VLAN. 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 second Gigabit port (configured as access mode):

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


Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88AB

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	2	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 22. VLAN PVID Configuration (Access)

CLI example – Set Port VLAN to 2 on the second Gigabit port (configured as trunk mode):

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

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

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

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88AB

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Trunk	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 23. VLAN PVID Configuration (Hybrid)

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 are tagged with a C-tag.

S-Port

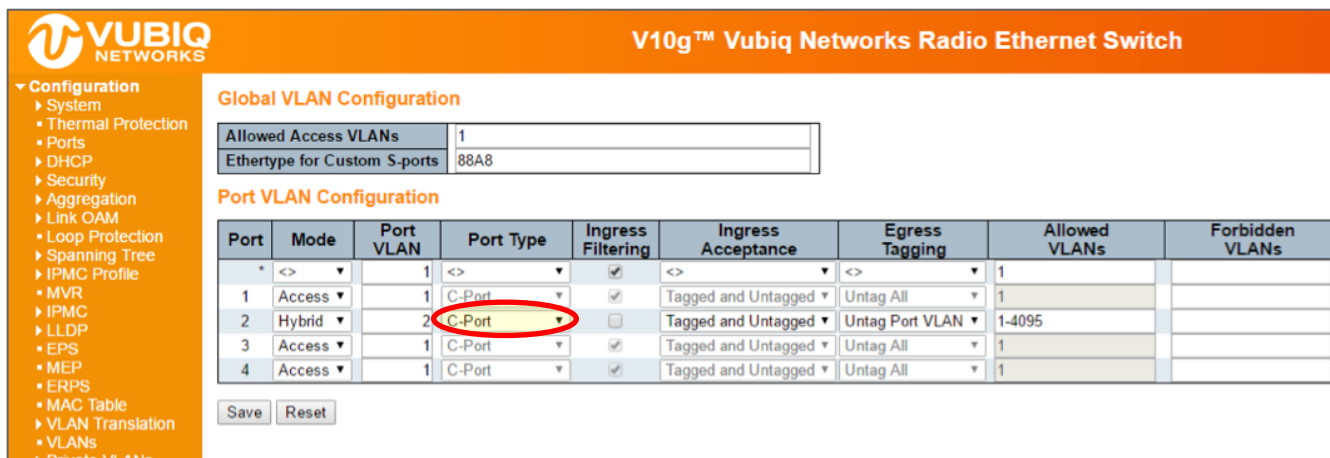
On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

S-Custom-Port

On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports 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 second Gigabit port:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(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.
(config-if)# switchport hybrid port-type c-port
(config-if)# exit
(config)# exit
#
```



The screenshot shows the configuration page for a Vubiq Networks V10g™ Vubiq Networks Radio Ethernet Switch. The page is divided into two main sections: Global VLAN Configuration and Port VLAN Configuration.

Global VLAN Configuration:

- Allowed Access VLANs: 1
- Ethertype for Custom S-ports: 88A8

Port VLAN Configuration:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Buttons: Save, Reset

Figure 24. VLAN Port Type Configuration

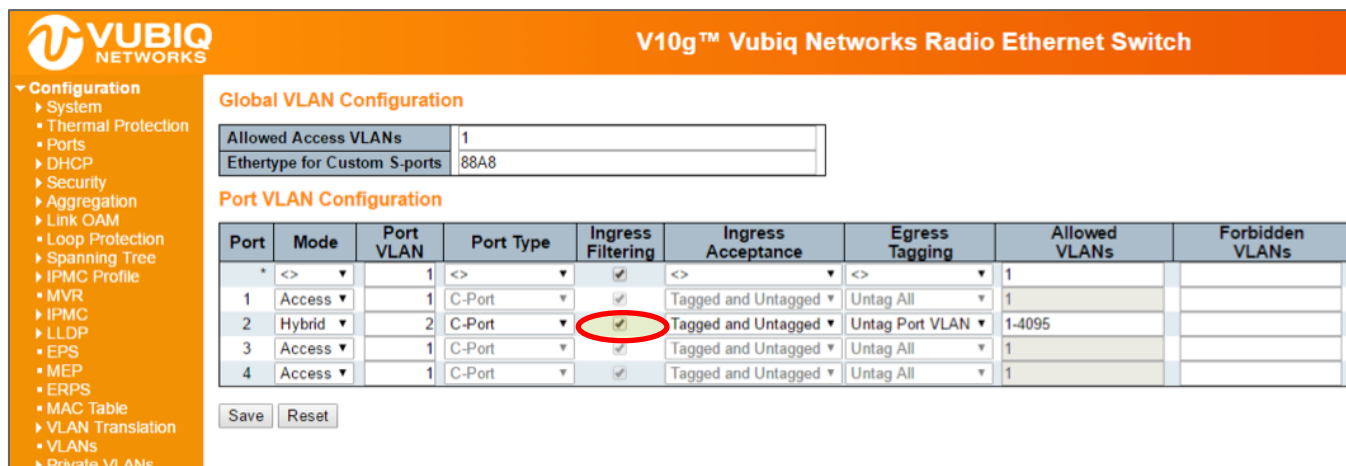
Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and trunk ports always have ingress filtering enabled. If ingress filtering is enabled, 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 second Gigabit port:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(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
(config-if)# switchport hybrid ingress-filtering
(config-if)# exit
(config)# exit
#
```



The screenshot shows the configuration page for a Vubiq Networks V10g™ Vubiq Networks Radio Ethernet Switch. The page is divided into two main sections: Global VLAN Configuration and Port VLAN Configuration.

Global VLAN Configuration:

- Allowed Access VLANs: 1
- Ethertype for Custom S-ports: 88A8

Port VLAN Configuration:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Buttons: Save, Reset

Figure 25. VLAN Ingress Filtering Configuration

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

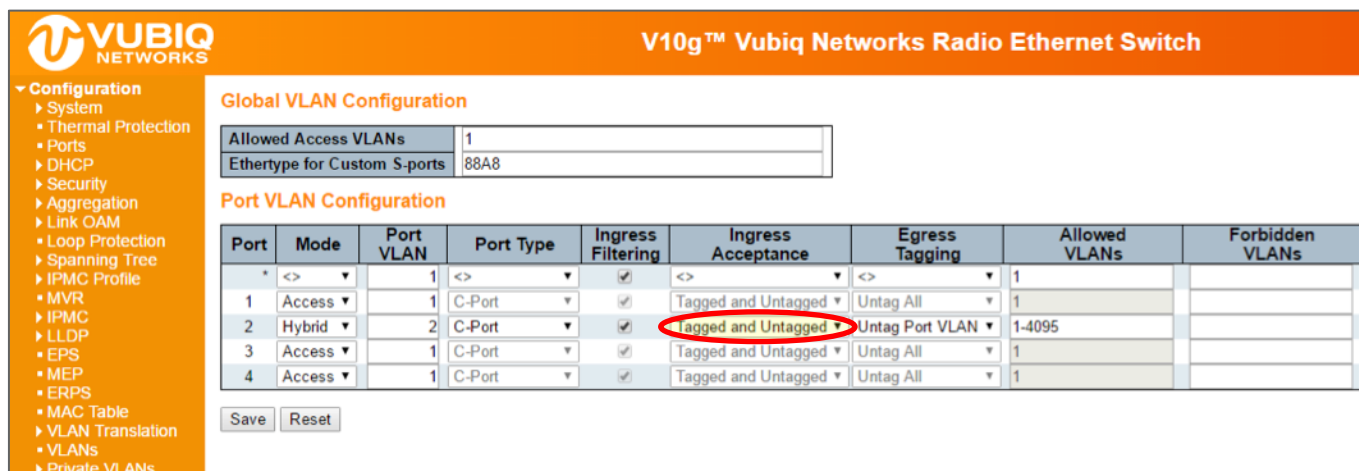
Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only

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

CLI example – configure ingress filtering on the second Gigabit port:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(config-if)# switchport hybrid acceptable-frame-type ?
    all           Allow all frames
    tagged        Allow only tagged frames
    untagged      Allow only untagged frames
(config-if)# switchport hybrid acceptable-frame-type all
(config-if)# exit
(config)# exit
#
```



The screenshot shows the configuration interface for a Vubiq Networks V10g switch. The 'Global VLAN Configuration' section includes fields for 'Allowed Access VLANs' (set to 1) and 'EtherType for Custom S-ports' (set to 88A8). The 'Port VLAN Configuration' section is a table with columns for Port, Mode, Port VLAN, Port Type, Ingress Filtering, Ingress Acceptance, Egress Tagging, Allowed VLANs, and Forbidden VLANs. The 'Ingress Acceptance' column for port 2 is circled in red, showing 'Tagged and Untagged'.

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Figure 26. VLAN Ingress Acceptance Configuration

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 second Gigabit port:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(config-if)# switchport hybrid egress-tag ?
    all           Tag all frames
    none          No egress tagging
(config-if)# switchport hybrid egress-tag none
(config-if)# exit
(config)# exit
#
```

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 27. VLAN Egress Tagging Configuration

Allowed VLANs

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

The field's syntax is identical to the syntax used in the Existing VLANs field. 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 second Gigabit port (configured as trunk mode):

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan ?
    <vlan_list>    VLAN IDs of the allowed VLANs when this port
                  is in trunk 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
(config-if)# switchport trunk allowed vlan 2
(config-if)# exit
(config)# exit
#
```

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

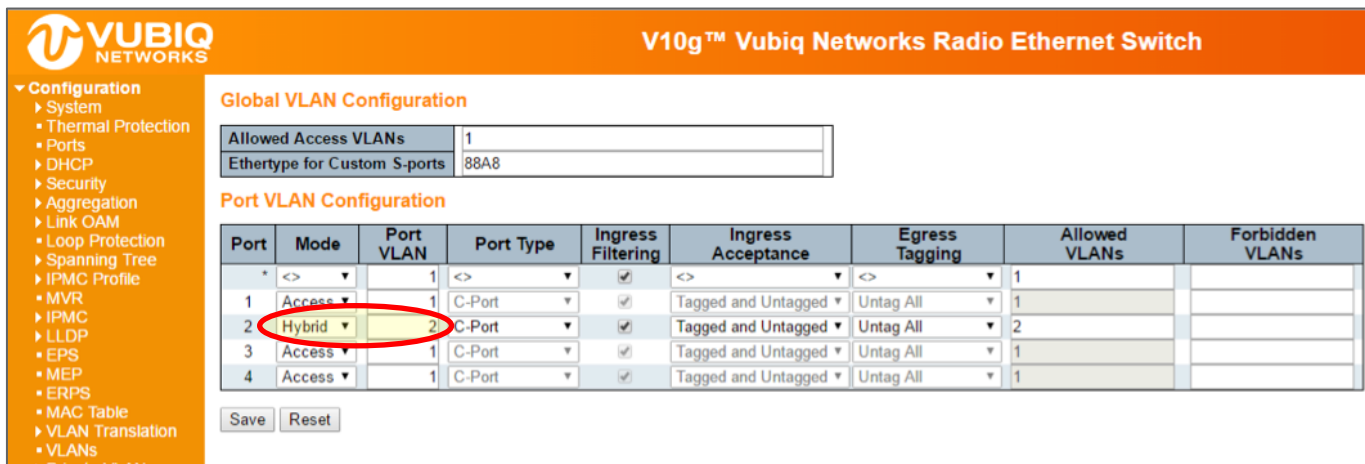
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Trunk	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 28. Allowed VLANs Configuration (Trunk)

CLI example – Set port VLAN to 2 on the second Gigabit port (configured as hybrid mode):

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



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	2	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

Figure 29. Allowed VLANs Configuration (Hybrid)

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 such as 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.

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 second Gigabit port:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
(config-if)# switchport forbidden vlan ?
  add      Add to existing list.
  remove  Remove from existing list.
(config-if)# switchport forbidden vlan add 5
(config-if)# exit
(config)# exit
#
```

 VUBIQ NETWORKS
V10g™ Vubiq Networks Radio Ethernet Switch

- ▼ Configuration
 - ▶ System
 - ▶ Thermal Protection
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Link OAM
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ EPS
 - ▶ MEP
 - ▶ ERPS
 - ▶ MAC Table
 - ▶ VLAN Translation
 - ▶ VLANs
 - ▶ Private VLANs

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Hybrid	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	2	5
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Figure 30. Forbidden VLANs Configuration

Show VLAN Status CLI example:

```
# show vlan ?
all          Show all VLANs (If left out only static VLANs
             are shown)
brief       VLAN summary information
id          VLAN status by VLAN id
ip-subnet   Show VCL 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>

# show vlan all
VLAN  Name                               Interfaces
----  -
1     default                               Gi 1/1,3-4
#
```

8.0 Generic VLAN Registration Protocol

Generic VLAN Registration Protocol (GVRP) is specified in IEEE 802.1Q-2005, clause 11 and IEEE 802.1D.2004, clause 12.

8.1 GVRP Port Configuration

GVRP is enabled on a port basis in the web GUI by going to **Configuration** → **GVRP** → **Port config**.

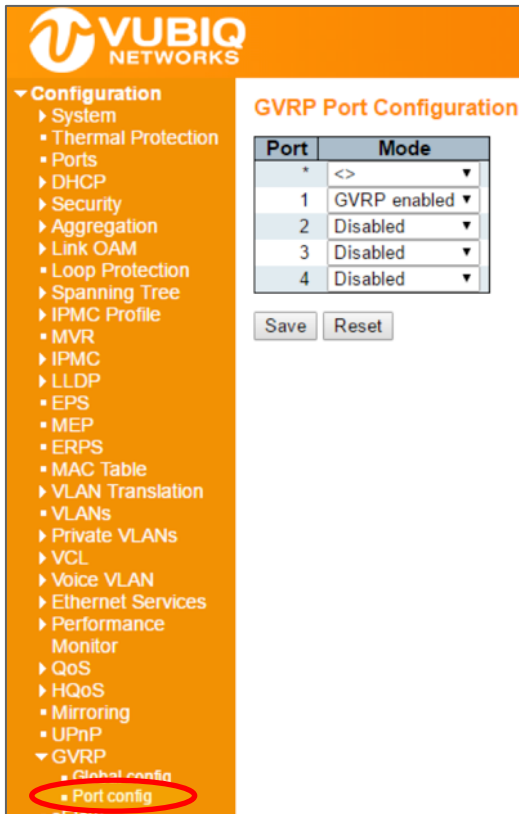


Figure 31. GVRP Port Configuration

The associated CLI command to enable GVRP is:

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

The associated CLI command to disable GVRP is:

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


8.2 Special Note for CEService

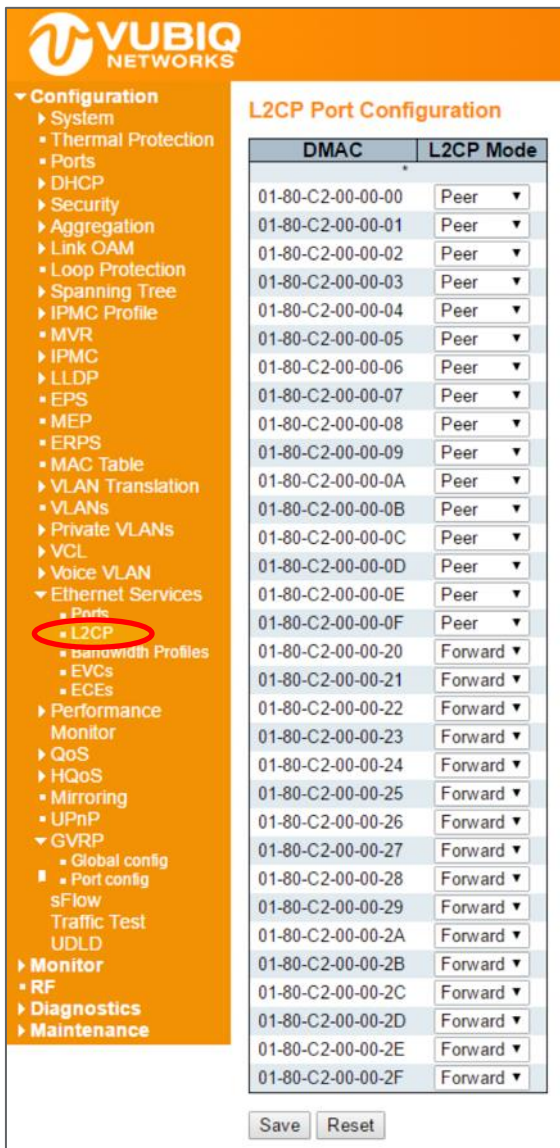
In general, this is enough for GVRP to work, however the CEService SDK allows the user to configure whether a L2CP (Layer 2 Control Protocol) is forwarded or sent to the CPU (peered). The default is forwarded.

When using CEService, the system must be told how GARP frames should be peered, as follows.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# gvrp
(config-if)# evc l2cp peer 17
(config-if)# exit
(config)# exit
#
```

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 to **Configuration > Ethernet Services > L2CP** and then select the port to configure in the upper right corner.



L2CP Port Configuration

DMAC	L2CP Mode
01-80-C2-00-00-00	Peer
01-80-C2-00-00-01	Peer
01-80-C2-00-00-02	Peer
01-80-C2-00-00-03	Peer
01-80-C2-00-00-04	Peer
01-80-C2-00-00-05	Peer
01-80-C2-00-00-06	Peer
01-80-C2-00-00-07	Peer
01-80-C2-00-00-08	Peer
01-80-C2-00-00-09	Peer
01-80-C2-00-00-0A	Peer
01-80-C2-00-00-0B	Peer
01-80-C2-00-00-0C	Peer
01-80-C2-00-00-0D	Peer
01-80-C2-00-00-0E	Peer
01-80-C2-00-00-0F	Peer
01-80-C2-00-00-20	Forward
01-80-C2-00-00-21	Forward
01-80-C2-00-00-22	Forward
01-80-C2-00-00-23	Forward
01-80-C2-00-00-24	Forward
01-80-C2-00-00-25	Forward
01-80-C2-00-00-26	Forward
01-80-C2-00-00-27	Forward
01-80-C2-00-00-28	Forward
01-80-C2-00-00-29	Forward
01-80-C2-00-00-2A	Forward
01-80-C2-00-00-2B	Forward
01-80-C2-00-00-2C	Forward
01-80-C2-00-00-2D	Forward
01-80-C2-00-00-2E	Forward
01-80-C2-00-00-2F	Forward

Save Reset

Figure 32. 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.

8.3 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 Configuration**.

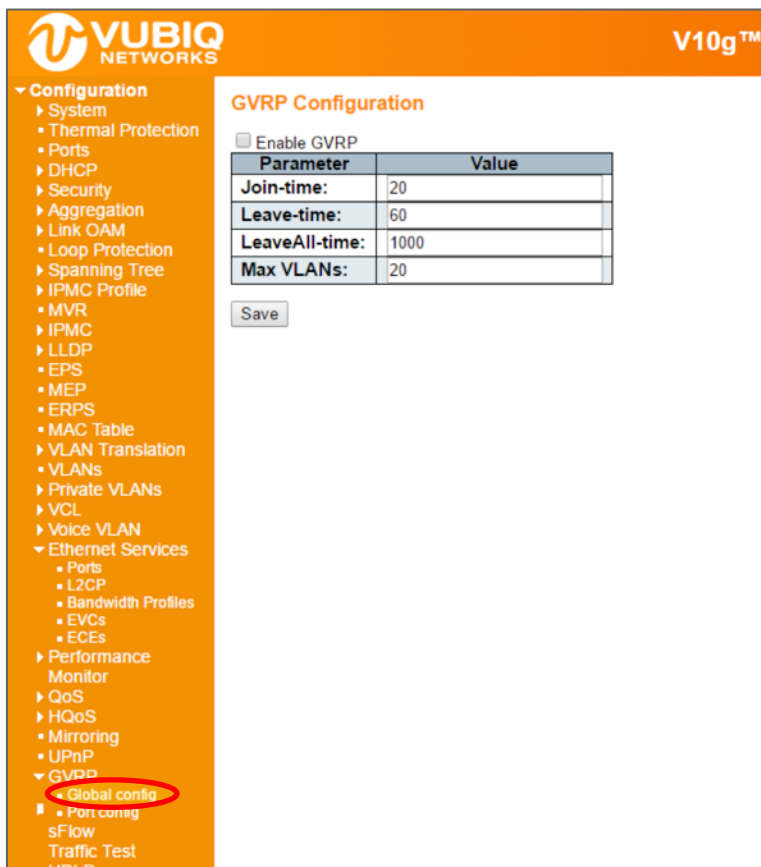


Figure 33. GVRP Global Configuration

The Enable GVRP checkbox enables GVRP globally.

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 puts the protocol parameter into its default value. The commands can also 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 puts an upper limit to the number resources that can be used.

Max VLANs is set to 20 when GVRP is enabled globally using the following command:

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

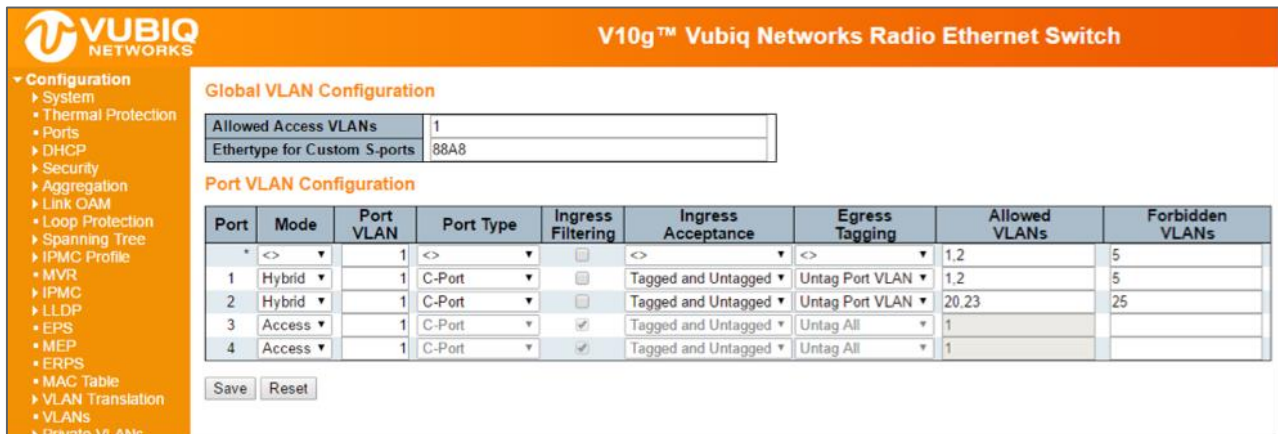
If a different value is needed, say 100, enable GVRP using the following command:

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

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

8.4 Fixed and Forbidden VLANs

The Fixed and Forbidden VLANs are configured from the VLAN menu by going to **Configuration > VLANs**.



Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input type="checkbox"/>	<>	<>	1,2	5
1	Hybrid	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1,2	5
2	Hybrid	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	20,23	25
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Figure 34. VLAN Table

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.

In the Registrar state 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
```

9.0 Multiple Spanning Tree Protocol

9.1 Bridge Settings

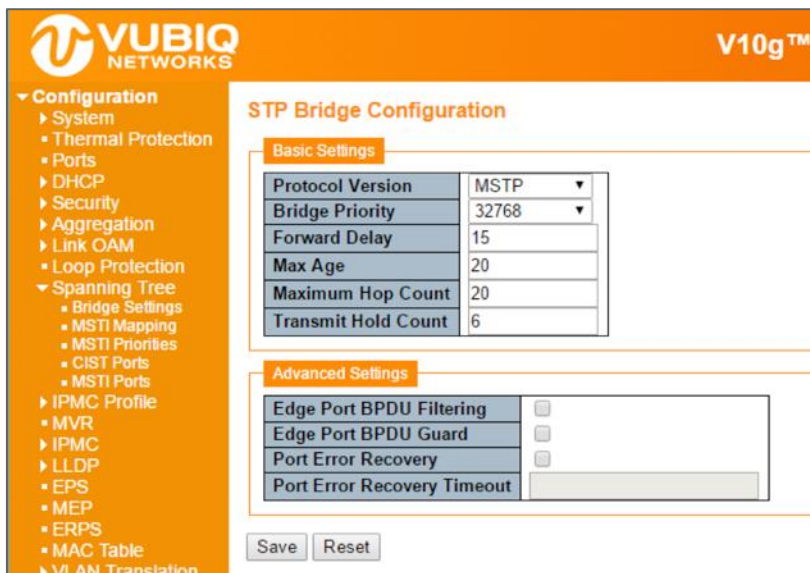


Figure 35. Bridge Setting

ICLI Commands for Basic Settings

The following ICLI commands refer to the basic settings. 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 $\langle 4096*i, i=0, \dots, 15 \rangle$ is one of the numbers $4096*i$, where $i=0, \dots, 15$. The *forward delay* is set by:

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

Where $\langle 4-30 \rangle$ 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>
```

ICLI Commands for Advanced Settings

The following ICLI commands refer to the advanced settings. 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
```

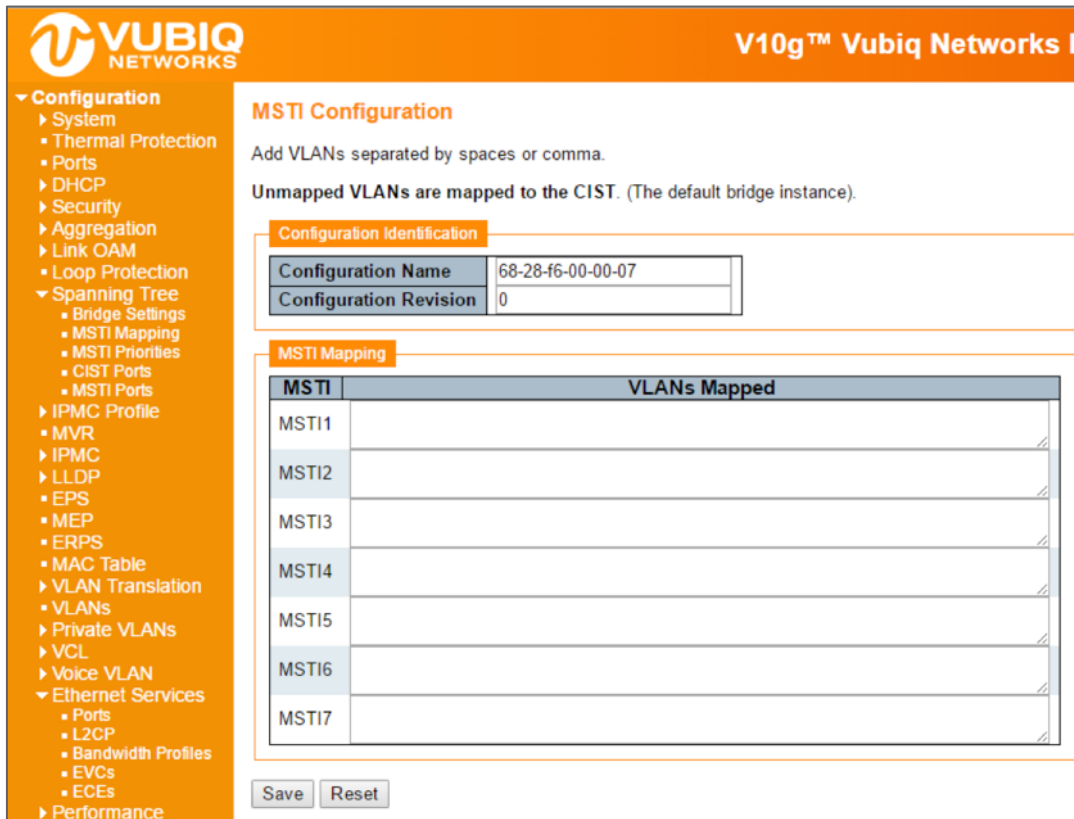
The *port error recovery* and *port error recovery timeout* is set by one ICLI command:

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

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

9.2 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. A MSTI configuration also has a name and revision. All these values have to be identical on the switches in the network. Otherwise the configuration will not take effect.



VUBIQ NETWORKS V10g™ Vubiq Networks F

Configuration

- System
 - Thermal Protection
 - Ports
- DHCP
- Security
- Aggregation
- Link OAM
 - Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
 - MVR
- IPMC
- LLDP
- EPS
- MEP
- ERPS
- MAC Table
- VLAN Translation
 - VLANs
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- Performance

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	68-28-f6-00-00-07
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save Reset

Figure 36. MSTI Configuration

The configuration identity is configured as follows:

```
(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.

The VLANs are added to MSTI1 and MIST2 with the following 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.

9.3 MSTI Priorities

Each MSTI and CIST can be given a priority.

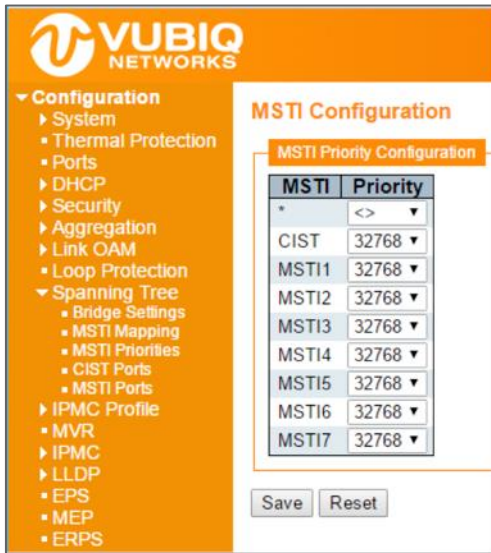


Figure 37. MSTI Priority Configuration

A low priority number indicates higher priority.

A *Bridge Identifier* is constructed per CIST, MSTI1,...,MSTI7, the bridge priority number. This is concatenated with the MAC address of the switch. In this way the bridge Identifier is unique.

A low bridge Identifier indicates a higher priority. A high priority means that the switch tends to be the root of the spanning tree. If two switches have the same bridge priority, then for example, setting MSTI1 priority higher, or setting MSTI2 lower, makes one switch tends the root.

9.4 STP CIST Port Configuration

STP is configured on a port basis in the web GUI at **Configuration > Spanning Tree > CIST Ports**.

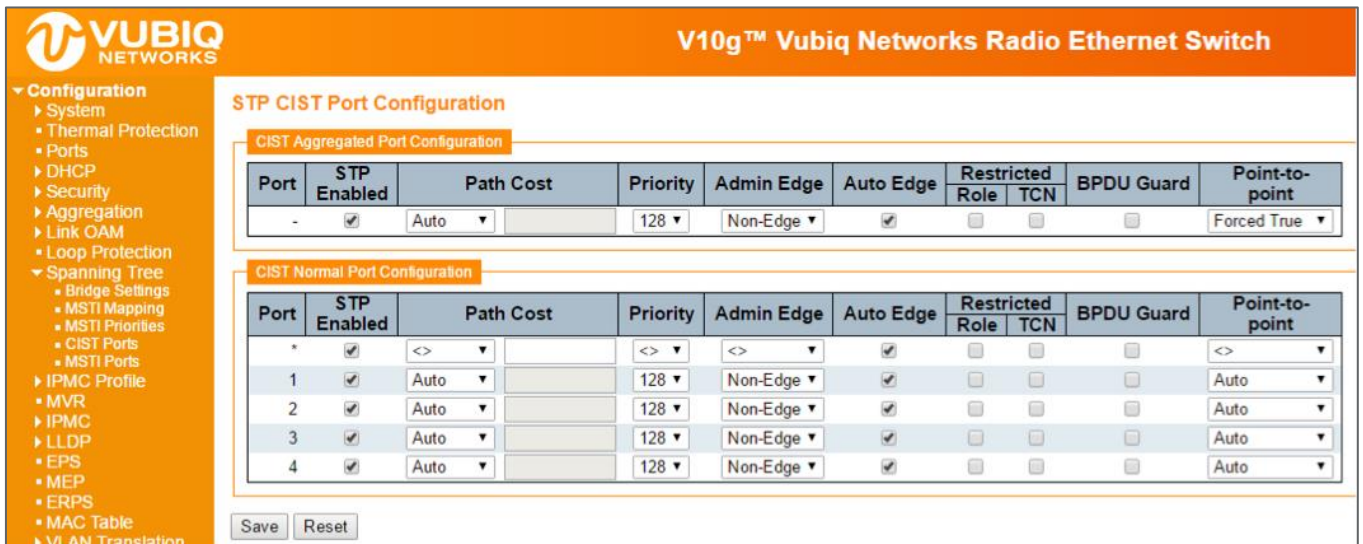


Figure 38. STP CIST Port Configuration

All parameters, except *Path Cost* and *Priority*, are specific for the port and not for CIST. These two parameters can be set for each MSTI, but the other parameters cannot because they apply to the port. If, for example, spanning tree is disabled (as it is for port 3), it applies to the CIST and all the MSTIs.

When using the ICLI, the *CIST Aggregation Port Configuration* commands are performed at the *Config* mode prompt as follows:

```
(config)#
```

The *CIST Normal Port Configuration* commands are performed in the *Config Interface* mode prompt as follows:

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

The following commands below assume that the user is in the interface config mode:

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
```

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>
```

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

<Priority> is a number in the range 0 to 240 and a multiple of 16. 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.

Admin Edge and Auto Edge

These two features are activated 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 is 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.

Restricted Role and Restricted TCN

These two features are activated 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.

BPDU Guard

This feature is activated the following ICLI command.

```
(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 portEdgeStatus does not affect this setting.

Point-to-Point

This feature is activated by the following ICLI command.

```
(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*.

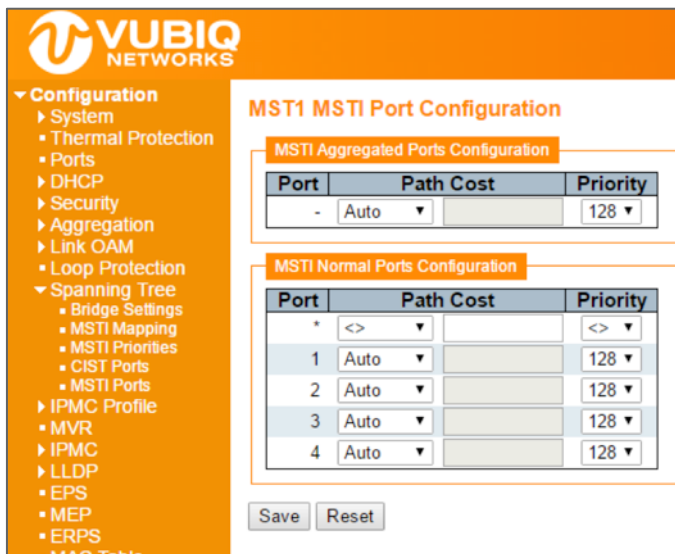
9.5 MSTI Ports

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



Figure 39. MSTI Port Configuration

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



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128

Save Reset

Figure 40. MST1 MSTI Port Configuration

The ICLI commands for setting the path cost and priority is the same as for CIST, 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.

<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.

<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.

10.0 RF Commands

There are a series of rf commands that can be executed at the CLI or through the Web GUI. The rf commands control how the rf or radio portion of the Vubiq HaulPass V10g work. Many of commands display data that is also available through SNMP. Where the data is available through SNMP the MIB and OID will be provided.

10.1 RF Board (Board Setting/Status)

The rf board commands allow the user to view the current values of several parameters but don't allow for the values to be changed.

current-5v (Board 5V current status)

The value reported by current-5v is the amount of current that the board is currently using in mA.

The CLI command:

```
# rf board current-5v
2388
#
```

The Web GUI view:

Board Measurements (Read Only)

Board Temp	52 C	Switch Temp	58 C
Tx Module Temp	50 C	Rx Module Temp	49 C
5V Current	4835 mA	Uptime	432571 seconds

MIB: vubiqRfBoardCurrent5V

OID: .1.3.6.1.4.1.46330.2.2.1.18.0 (Integer)

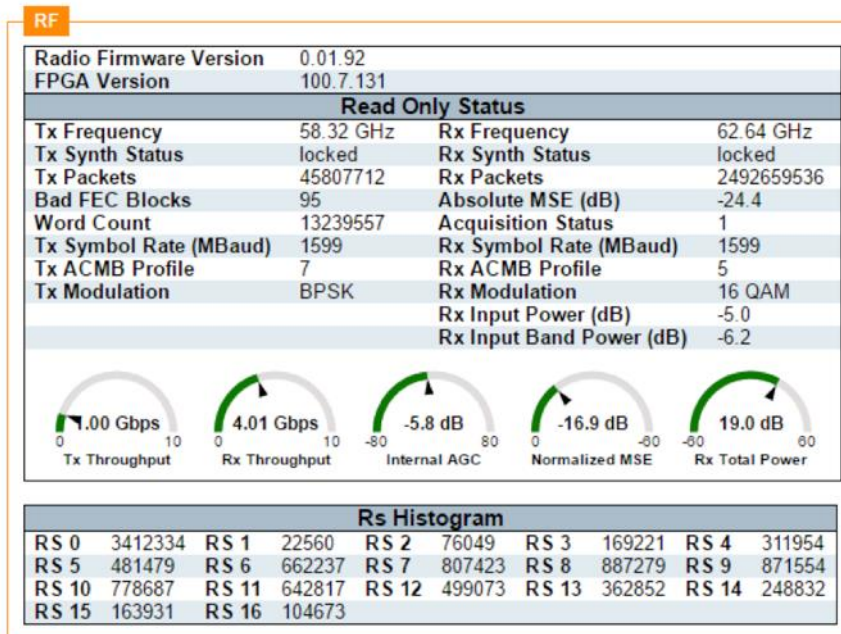
firmware version (Board firmware version setting)

The value reported by the firmware command is the revision of the current RF firmware.

The CLI command:

```
# rf board firmware version
2.03.05
#
```

The Web GUI view:



MIB: vubiqRfFirmwareVersion

OID: .1.3.6.1.4.1.46330.2.2.1.20.0 (OctetString)

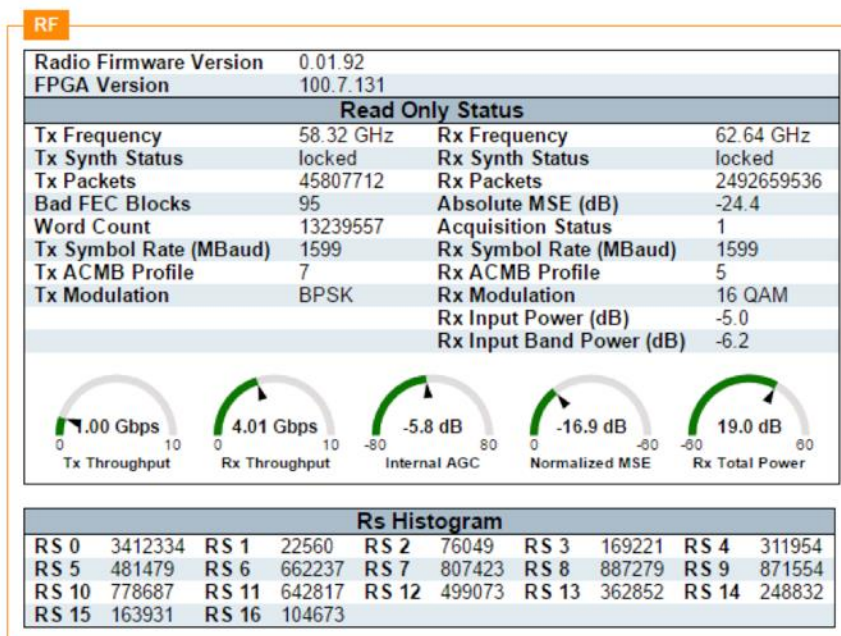
fpga (Board FPGA version setting)

The value reported by the fpga command is the revision of the current RF fpga.

The CLI command:

```
# rf board fpga version
96
#
```

The Web GUI view:



MIB: vubiqRfPpgaVersion

OID: .1.3.6.1.4.1.46330.2.2.1.21.0 (OctetString)

temp (Board temperature setting)

The temp parameter shows the current operating temperature of the Vubiq HaulPass V10g.

The CLI command:

```
# rf board temp
0
#
```

The Web GUI view:

Board Measurements (Read Only)			
Board Temp	52 C	Switch Temp	58 C
Tx Module Temp	50 C	Rx Module Temp	49 C
5V Current	4835 mA	Uptime	432571 seconds

MIB: vubiqRfBoardTemp

OID: .1.3.6.1.4.1.46330.2.2.1.15.0 (Integer)

uptime (Board uptime status)

The uptime measures the amount of uptime measured in seconds that RF Subsystem has this power cycle.

The CLI command:

```
# rf board uptime
5421
#
```

The Web GUI:

Board Measurements (Read Only)			
Board Temp	52 C	Switch Temp	58 C
Tx Module Temp	50 C	Rx Module Temp	49 C
5V Current	4835 mA	Uptime	432571 seconds

MIB: vubiqRfBoardUpTime

OID: .1.3.6.1.4.1.46330.2.2.1.19.0 (Integer)

10.2 rf rx (Rx Module Command)

agc-sensitivity (Rx AGC sensitivity setting)

The agc-sensitivity command allows the user to read and write the receive agc-sensitivity of the RF receive module.

CLI example:

```
# rf rx agc-sensitivity 16
# rf rx agc-sensitivity
16
#
```

MIB: vubiqRfRxAgcSensitivity

OID: .1.3.6.1.4.1.46330.2.2.1.14.0 (Integer)

auto-atten (Rx auto-atten setting/status)

The auto-atten setting is a switch that enables firmware auto attenuation when it is a 1 and disables firmware auto attenuation when it is a 0. The seek-status informs the user as to whether the auto attenuation has settled on a value or is looking for a working value.

CLI example:

```
# rf rx auto-atten mode 1
# rf rx auto-atten mode
1
# rf rx auto-atten seek-status
seeking
#
```

Web GUI:

Board Settings			
Tx IF Atten (dB)	13.3 ▼	Rx BB Atten (dB)	24
Rx IF Atten (dB)	5.3 ▼	Auto Atten Mode	1 ▼
Mode	2.5 ▼	Test Tone (MHz)	0

MIB: vubiqRfRxAutoAttenMode

OID: .1.3.6.1.4.1.46330.2.2.1.12.0 (Integer)

bb atten (Rx BB atten setting)

The bb atten setting allows the user to read and write the BB attenuation setting. It can have a value of 1 or 2.

CLI example:

```
# rf rx bb atten ?
<1-2> Atten select. One of { 1 | 2 }
# rf rx bb atten 1
0
# rf rx bb atten 2
0
#
```

Web GUI example:

Board Settings			
Tx IF Atten (dB)	13.3 ▼	Rx BB Atten (dB)	24
Rx IF Atten (dB)	5.3 ▼	Auto Atten Mode	1 ▼
Mode	2.5 ▼	Test Tone (MHz)	0

MIB: vubiqRfRxBbAtten1

OID: .1.3.6.1.4.1.46330.2.2.1.10.0 (Integer)

MIB: vubiqRfRxBbAtten2

OID: .1.3.6.1.4.1.46330.2.2.1.11.0 (Integer)

dssi (Rx DSSI status)

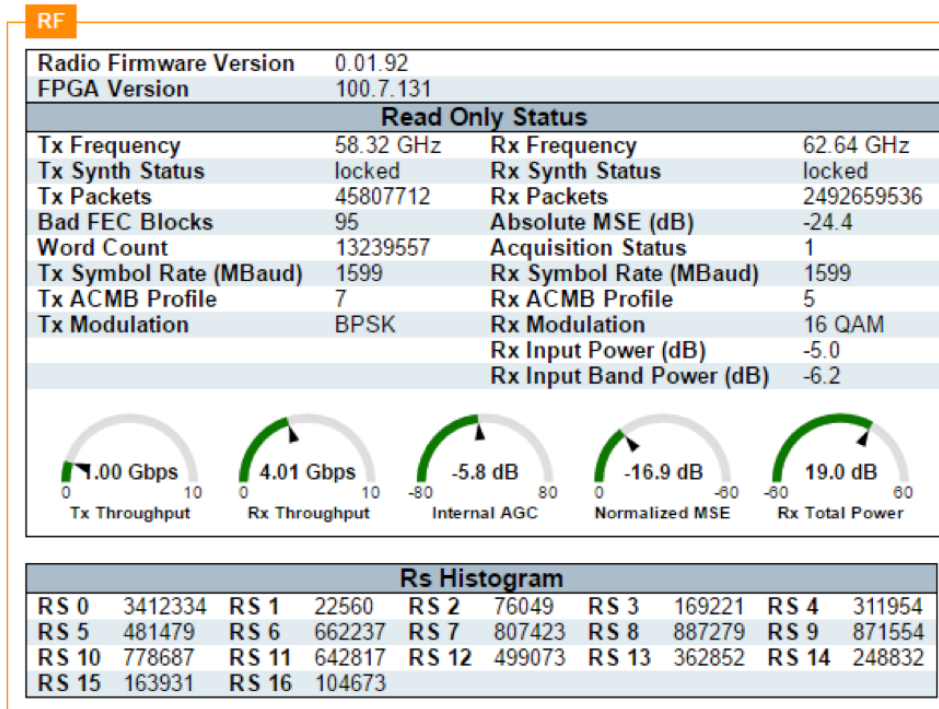
DSSI or Digital Signal Strength Indication is an overall goodness measurement of the quality of the digital data being received across the radio link. The DSSI is nominally 100 but occasional blips below 90 are not necessarily

an indicator of problems. Vubiq recommends watching for a sustained degradation of DSSI below 90 for two minutes or more.

CLI example:

```
# rf rx dssi
0
#
```

Web GUI example:



MIB: vubiqRfDssi

OID: .1.3.6.1.4.1.46330.2.2.1.7.0 (Integer)

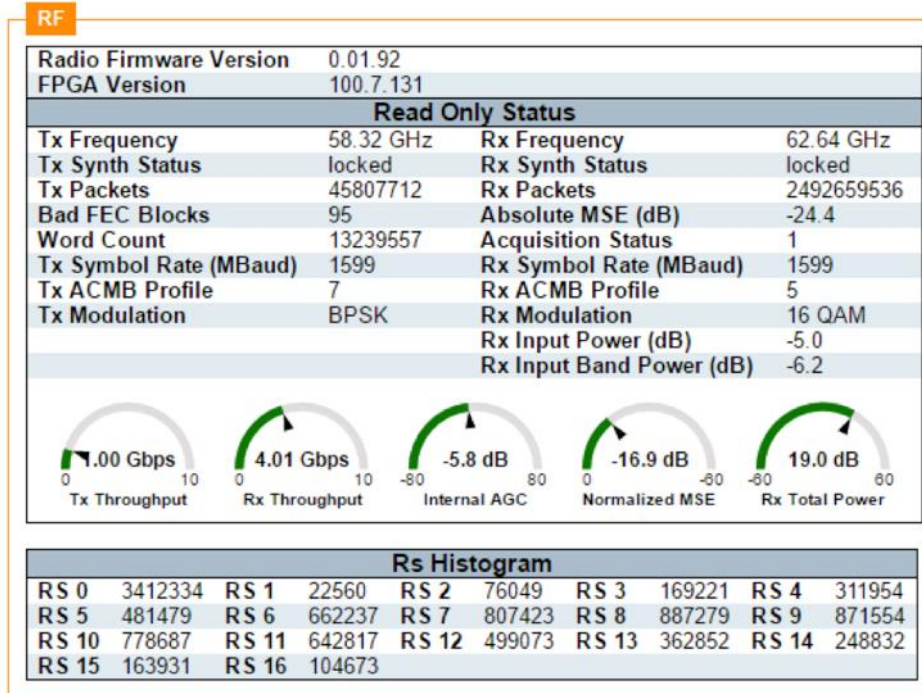
```
errors          Rx error status
```

There are two types of errors that the Vubiq HaulPass V10g can report, FEC or Forward Error Correction errors and uncorrectable errors that had to be retransmitted across the radio link.

CLI example:

```
# rf rx errors ?
    fec          Rx FEC error status
    uncorrectable Rx uncorrectable error status
# rf rx errors fec
0
# rf rx errors uncorrectable
0
#
```

Web GUI example:



MIB: vubiqRfRxFecErrors

OID: .1.3.6.1.4.1.46330.2.2.1.23.0 (Counter32)

MIB: vubiqRfRxUncorrectableErrors

OID: .1.3.6.1.4.1.46330.2.2.1.6.0 (Integer)

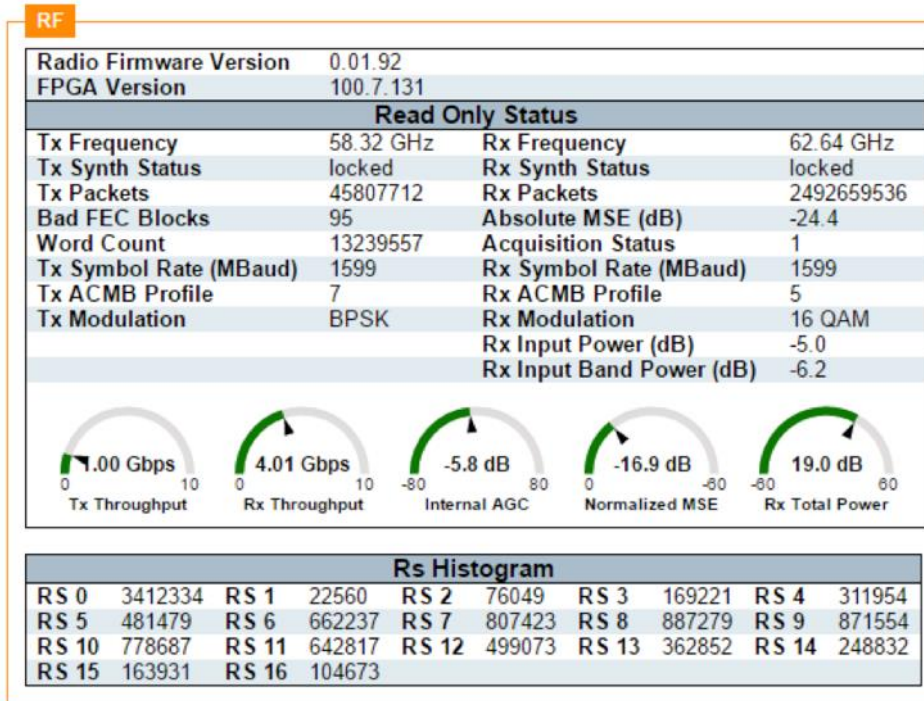
freq (Rx frequency setting (GHz))

The rf rx freq command will tell the user which frequency the Vubiq HaulPass V10g terminal is receiving at. The receiver and transmitter frequencies must be different and the terminal at the other end of the link must reverse those frequencies in order to have a link between them. Transmitting at 57.78 GHz makes the terminal a “Low” and transmitting at 64.26 GHz makes the terminal a “High”.

CLI example:

```
# rf rx freq
64.26
# rf tx freq
57.78
#
```

Web GUI example:



MIB: vubiqRfRxFreq

OID: .1.3.6.1.4.1.46330.2.2.1.3.0 (Integer)

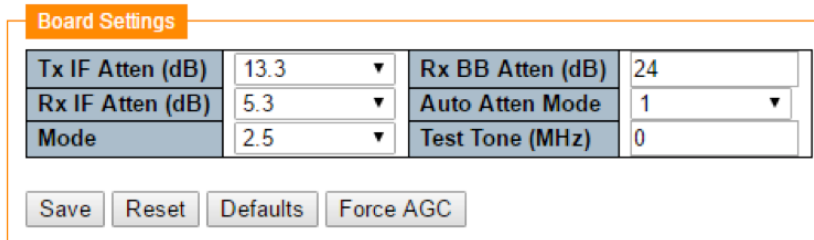
if (Rx IF atten setting)

The Receiver IF attenuation setting can be discovered through the RF RX IF Atten setting. The value is in dB.

CLI example:

```
# rf rx if atten ?
  <word>      Atten value in dB.  One of { 0 | 1.3 | 2.7 | 4.0 | 5.3 | 6.7 |
              8.0 | 9.3 | 10.7 | 12.0 | 13.3 | 14.7 | 16.0 | 17.3 | 18.7 | 20.0
              }
  <cr>
# rf rx if atten 8.0
# rf rx if atten
8.0
#
```

Web GUI example:



MIB: vubiqRfRxIfAtten

OID: .1.3.6.1.4.1.46330.2.2.1.9.0 (Integer)

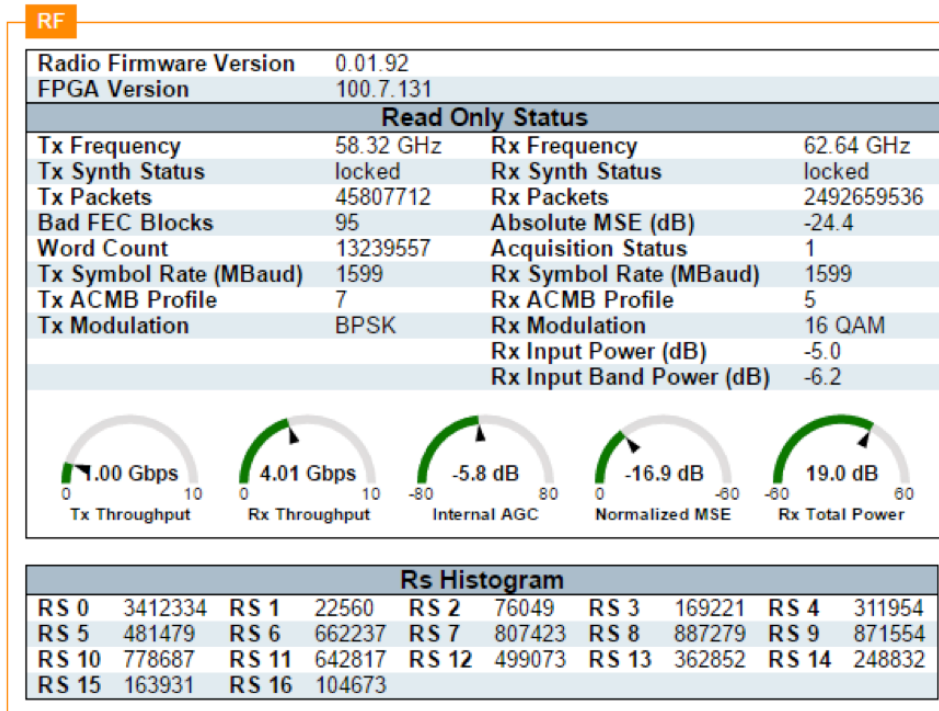
sync (Rx sync status)

The RF Rx sync status is a gauge that ranges from 0 (no sync) to 40 (perfect sync).

CLI example:

```
# rf rx sync ?
  <0-40>   Sync status (0: No sync, 40: Perfect sync)
  <cr>
# rf rx sync
0
#
```

Web GUI example:



MIB: vubiqRfRxSync

OID: .1.3.6.1.4.1.46330.2.2.1.5.0 (Integer)

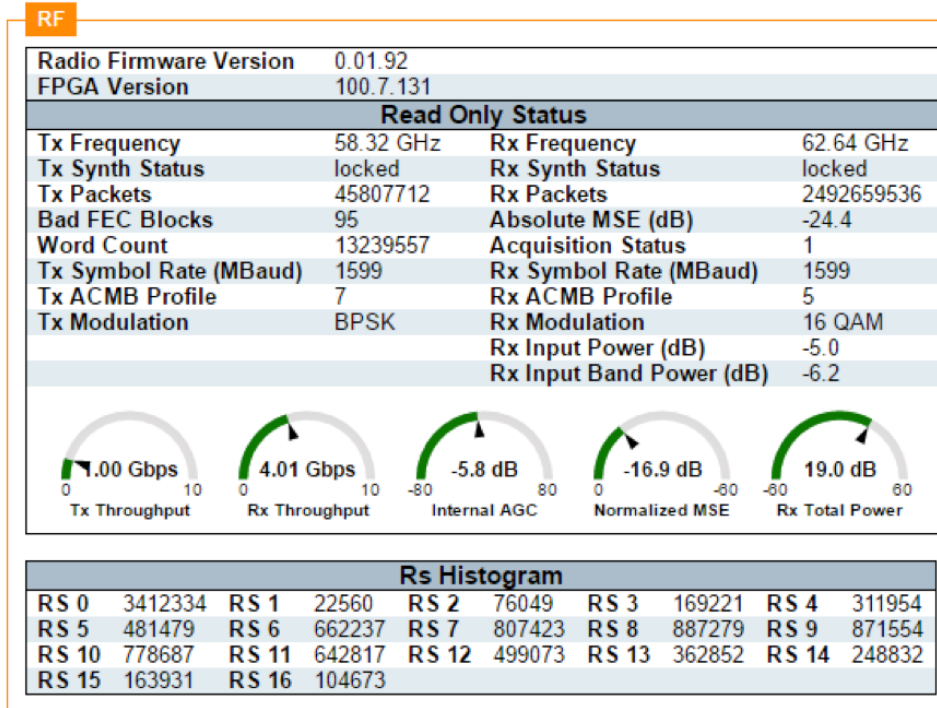
synth (Rx synth status)

The rf rx synth status tells the user the status of the RF Receive frequency synthesizer or Phase Locked Loop. The values that it can have are high, low, locked, or invalid. A normally operating unit should be locked.

CLI example:

```
# rf rx synth status ?
  <word>   Synth status. One of { high | low | locked | invalid }
  <cr>
# rf rx synth status
locked
#
```

Web GUI example:



MIB: vubiqRfRxSynthStatus

OID: .1.3.6.1.4.1.46330.2.2.1.4.0 (Integer)

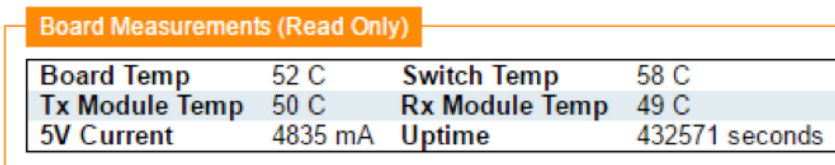
temp (Rx temperature setting)

The RF RX Temp setting tells the user the temperature of the RF Receiver in degrees C.

CLI example:

```
# rf rx temp ?
  <int>   Temperature in deg C.
  <cr>
# rf rx temp
0
#
```

Web GUI example:



MIB: vubiqRfRxTemp

OID: .1.3.6.1.4.1.46330.2.2.1.17.0 (Integer)

10.3 rf tx (RF Tx Module Setting/Status)

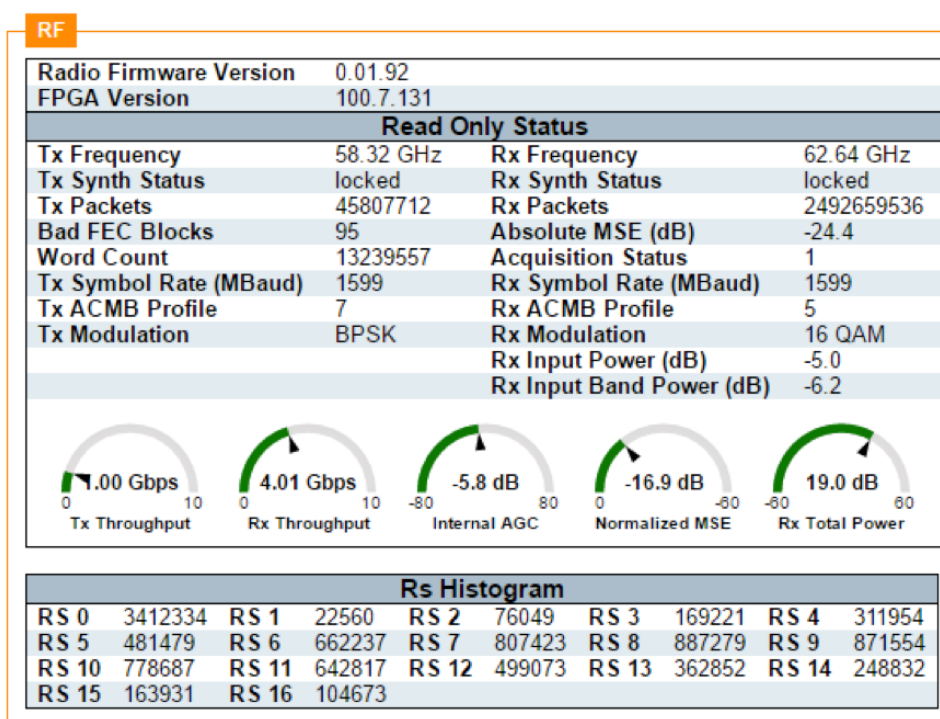
freq (Tx frequency setting (GHz))

The rf tx freq command will tell the user which frequency the Vubiq HaulPass V10g terminal is transmitting at. The receiver and transmitter frequencies must be different and the terminal at the other end of the link must reverse those frequencies in order to have a link between them. Transmitting at 57.78 GHz makes the terminal a “Low” and transmitting at 64.26 GHz makes the terminal a “High”.

CLI example:

```
# rf rx freq
64.26
# rf tx freq
57.78
#
```

Web GUI example:



MIB: vubiqRfTxFreq

OID: .1.3.6.1.4.1.46330.2.2.1.1.0 (Integer)

if (Tx IF atten setting)

The Transmitter IF attenuation setting can be discovered through the RF TX IF Atten setting. The value is in dB.

CLI example:

```
# rf tx if atten ?
<word>      Atten value in dB. One of { 0 | 1.3 | 2.7 | 4.0 | 5.3 | 6.7 | 8.0
            | 9.3 | 10.7 | 12.0 | 13.3 | 14.7 | 16.0 | 17.3 | 18.7 | 20.0 }
<cr>
# rf tx if atten 4.0
# rf tx if atten
4.0
#
```

Web GUI example:

Board Settings

Tx IF Atten (dB)	13.3	Rx BB Atten (dB)	24
Rx IF Atten (dB)	5.3	Auto Atten Mode	1
Mode	2.5	Test Tone (MHz)	0

MIB: vubiqRfTxIfAtten

OID: .1.3.6.1.4.1.46330.2.2.1.8.0 (Integer)

synth (Tx synth status)

The rf tx synth status tells the user the status of the RF Transmit frequency synthesizer or Phase Locked Loop. The values that it can have are high, low, locked, or invalid. A normally operating unit should be locked.

CLI example:

```
# rf tx synth status ?
    <word>    Synth status.  One of { high | low | locked | invalid }
    <cr>
# rf tx synth status
Locked
#
```

Web GUI example:

RF

Radio Firmware Version	0.01.92		
FPGA Version	100.7.131		
Read Only Status			
Tx Frequency	58.32 GHz	Rx Frequency	62.64 GHz
Tx Synth Status	locked	Rx Synth Status	locked
Tx Packets	45807712	Rx Packets	2492659536
Bad FEC Blocks	95	Absolute MSE (dB)	-24.4
Word Count	13239557	Acquisition Status	1
Tx Symbol Rate (Mbaud)	1599	Rx Symbol Rate (Mbaud)	1599
Tx ACMB Profile	7	Rx ACMB Profile	5
Tx Modulation	BPSK	Rx Modulation	16 QAM
		Rx Input Power (dB)	-5.0
		Rx Input Band Power (dB)	-6.2

Tx Throughput

Rx Throughput

Internal AGC

Normalized MSE

Rx Total Power

Rs Histogram									
RS 0	3412334	RS 1	22560	RS 2	76049	RS 3	169221	RS 4	311954
RS 5	481479	RS 6	662237	RS 7	807423	RS 8	887279	RS 9	871554
RS 10	778687	RS 11	642817	RS 12	499073	RS 13	362852	RS 14	248832
RS 15	163931	RS 16	104673						

MIB: vubiqRfTxSynthStatus

OID: .1.3.6.1.4.1.46330.2.2.1.2.0 (Integer)

temp (Tx temperature setting)

The RF TX Temp setting tells the user the temperature of the RF Transmitter in degrees C.

CLI example:

```
# rf tx temp ?
    <int>      Temperature in deg C.
    <cr>
# rf tx temp
0
#
```

Web GUI example:

Board Measurements (Read Only)

Board Temp	52 C	Switch Temp	58 C
Tx Module Temp	50 C	Rx Module Temp	49 C
5V Current	4835 mA	Uptime	432571 seconds

MIB: vubiqRfTxTemp

OID: .1.3.6.1.4.1.46330.2.2.1.16.0 (Integer)



Making Millimeter Wave Ubiquitous

Vubiq Networks, Inc.
9231 Irvine Blvd, Irvine, CA 92618 USA
www.vubiqnetworks.com