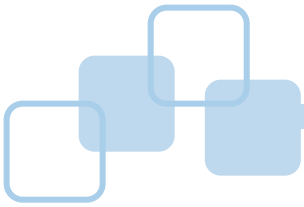


USER'S MANUAL

G.SHDSL Termination Unit

Comet 16xF/FM and 160xF-R/ FM-R

Version: 1.6

Date: 2023/08/08

Headquarters:
3F, No.108, Ruiquang Rd.,
Neihu Dist., Taipei 114,
Taiwan
TEL: 886-2-26583000
FAX: 886-2-27938000

Notice

This document is protected by the international copyright law. No part of this publication may be reproduced by any means without the permission of TAINET Communication System Corporation.

TAINET is a registered trademark, and Comet 160xF/ FM and Comet 160xF-R/ FM-R Series is a trademark of TAINET Communication System Corporation.

Other product names mentioned in this manual are used for identification purposes only and may be trademarks or trademarks of their respective companies.

The information provided from TAINET Communication System Corporation is believed to be accurate. Any changes and enhancements to the product and to the information thereof will be documented and issued as a new release to this manual.

Trademark

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

CE COMPLIANCE

This is to certify that the product listed below was tested in the laboratory to comply with the required criteria levels of the follow-mentioned Generic Standards or Product Family Standard(s) and/or Basic Standard(s) based-on the essential conformity requirements of EMC Directive 2014/30/EU.

Certification:

Formerly **CE mark**

Safety:

EN 62368-1, IEC 62368-1

EMC:

CISPR 32, EN 55032, EN 55035, EN 61000-3-2,
EN 61000-3-3, EN50121-4(for Comet 1602F-R/1604F-R/1608F-R)

ISO 9001 Quality Management

About This Manual

This section guides you on how to use the manual effectively. The manual contains information needed to install, configure, and operate TAINET's Comet 160xF/ FM and Comet 160xF-R/ FM-R Series termination units. The summary of this manual is as follows:

Chapter 1: Overview

Describe Comet 160xF/ FM and Comet 160xF-R/ FM-R Series in several applications.

Chapter 2: Specifications

Describe the features, specifications and applications of Comet 160xF/ FM and Comet 160xF-R/ FM-R Series.

Chapter 3: Interfaces

Introduce all the interfaces, including front panel and rear pane of Comet 160xF/ FM and Comet 160xF-R/ FM-R Series.

Chapter 4: Installation

Assist user to install and verify the Comet 160xF/ FM and Comet 160xF-R/ FM-R Series step-by-step.

Chapter 5: Operation of Web

Give a description of the Web Interface.

Chapter 6: Operation of CID

Give a description of the CID (Craft Interface Device).

Appendix A: Pin Assignment

The description of pin assignment

Appendix B: Trouble Report

Trouble Report Form

Symbols Used in This Manual

3 types of symbols are used throughout this manual. These symbols are used to advise the users when a special condition arises, such as a safety or operational hazard, or to present extra information to the users. These symbols are explained below:

Warning:

This symbol and associated text are used when death or injury to the user may result if operating instructions are not followed properly.

Caution:

This symbol and associated text are used when damages to the equipment or impact to the operation may result if operating instructions are not followed properly.

Note:

This symbol and associated text are used to provide the users with extra information that may be helpful when following the main instructions in this manual.

LIMITED WARRANTY

TAINET's DISTRIBUTOR shall be responsible to its customers for any and all warranties, which it makes relating to Products, and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory. TAINET warrants to DISTRIBUTOR that the Products to be delivered hereunder will be free of defects in material and workmanship under normal use and service for a period of twenty-four (24) months [twelve (12) months in Taiwan] following the date of shipment to DISTRIBUTOR.

If during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR notifies TAINET of such defect within seven days after knowing of such defect, TAINET shall, for any Product that TAINET agrees is defective, at its option, supply a replacement part, request return of equipment to its plant for repair, or perform necessary repair at the equipment's location. At TAINET's option, DISTRIBUTOR shall destroy any Product that TAINET agrees is defective and shall provide satisfactory proof of such destruction to TAINET. TAINET is not responsible for Products damaged by misuse, neglect, accident, or improper installation, or if repairs or modifications were made by persons other than TAINET's own authorized service personnel, unless such repairs by others were made with the written consent of TAINET.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties that extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall TAINET be liable for consequential damages. If distributor extends to its customers any additional warranty with respect to Products that is broader in scope than the warranty provided by TAINET, DISTRIBUTOR shall be solely responsible for any and all liabilities, obligations and damages resulting from the extension of such warranty.

TAINET shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits, from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance, or use of the Products, and in no event shall TAINET's liability exceed the purchase price of the Products.

Software Products are provided "as is" and without warranty of any kind. TAINET disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. TAINET shall not be liable for any loss of use, interruption of business or indirect, special, incidental, or consequential damages of any kind. TAINET shall do its best to provide end users with Software updates during the warranty period under this Agreement.

TAINET has not been notified of any intellectual property rights or others which may be infringed by the Products or the promotion, marketing, sale (or resale), or servicing thereof in the Territory, but TAINET makes NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT THERETO.

CONTENTS

FIGURES

TABLES

Chapter 1. Overview

This chapter begins with a general description of Comet 16xxF/160xFM Series and Comet 160xF-R/ FM-R Series. Then it describes how to use TAINET Comet Series in several applications.

1.1 Overview

DSL (Digital Subscriber Loop) technologies utilize the bandwidth capacity of existing ubiquitous telephone line (the local copper loops). G.SHDSL is designed for business applications, where high speed is required for full duplex transmission directions. It provides symmetrical data rates from 192Kbps to 5.696Mbps in 2-wire with a transmission distance up to 10Kft using SHDSL technology. With the proprietary TC-PAM technology, the maximum data rate may extend to 15.232Mbps on 2-wire mode. The data rates will be increased to 30.464Mbps in 4-wire link and 60.932Mbps in 8-wire link. The speed's obtainable using DSL bonding technologies are tied to the distance between the customer premise and the Telco central office. Performance varies with loop characteristics, such as line conditions, loop distance, wire gauge, noise, the line pairs and locations of bridged taps and gauge changes. The G.SHDSL bit rate can be configured (or rate adapted) to adapt to the line conditions.

The Comet 160xF/ FM series and Comet 160xF-R/ FM-R series are G.SHDSL.bis transmission equipment that using EFM/ATM/PTM frame to do Ethernet extension. The Comet 160xFM has a dual or quadruple link for ring or linear network connection. These G.SHDSL NTUs provide local/ remote loopback functions between two devices, by using EOC in between local and remote sides, can do system configuration, testing, performance and alarm monitoring of DSL link. It is very convenient for network testing and maintenance.

1.2 Applications

The SHDSL System consists of a central unit, CO (SHDSL Transceiver Unit – for Central Office), at central office, and a remote unit, CPE (SHDSL Transceiver Unit – for Customer Premise Equipment), at customer premises.

The services are extended through the ubiquitous copper wires or leased lines with the technologies of G.SHDSL. Ethernet interface extensions are supported on Comet 160xF/ FM and Comet 160xF-R/ FM-R. Figure 1-1 shows a typical back to back application.

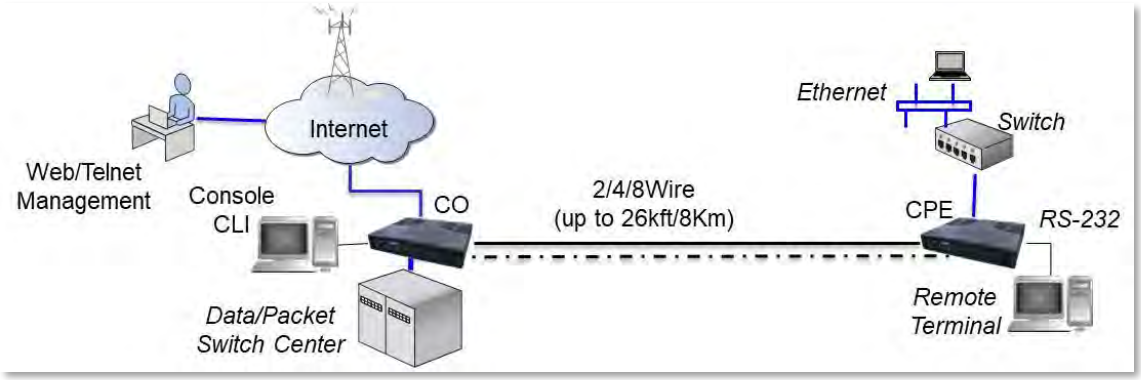


Figure 1-1 Application of Back-to-back

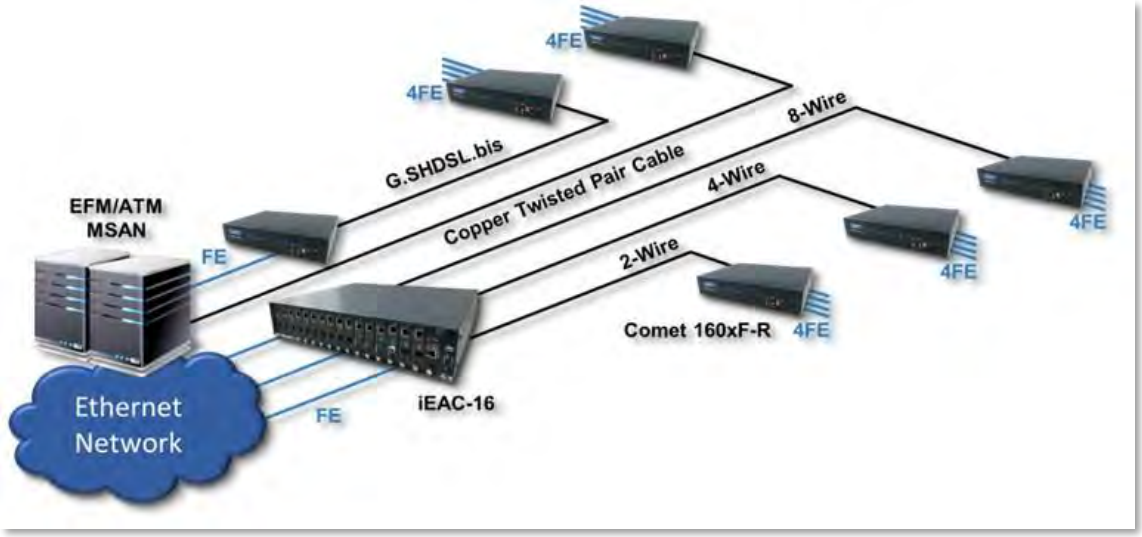


Figure 1-2 Application of Comet 160xF series modem

Chapter 2. Specification

To lead the user understand the TAINET Comet Series, this chapter begins with its main features. Then it continues to present SHDSL and G.SHDSL.bis interface, the network side interface, timing and synchronization, OAM (Operation, Administration and Maintenance) and technical specifications. The last part of this chapter is devoted to the applications of TAINET Comet 160xF/ FM Series in different networks.

2.1 Main Features

Listed below are the main features of the Comet 160xF/ FM and 160xF-R/ FM-R Series:

- Comet 160xF and 160xF-R/ FM-R series support EFM and ATM Point-to-point mode
- Comet 160xFM support EFM P2P (Point-to-point) or P2MP (point-to-multipoint) mode for party line linear link, ring, or star topology
- EFM mode complies with ITU-T G991.2 standard, TC-PAM 4/8/16/32/64/128 line-coding and IEEE 802.3ah 2Base-TL bonding
- ATM mode complies with RFC 1483 and RFC 2684 Multiprotocol over AAL5 bridge mode
- Carrying symmetrical 5.696 Mbps, 11.392Mbps, 22.784Mbps for up to 1.8 miles / 3 Km over 24-AWG (0.5mm) single pair copper wire
- Automatic line rate selection with Line Probe enabled
- Support SHDSL and SHDSL.bis payload rates of n×64Kbps, where n is 3 to 89 in 2 wires, n is 6 to 178 in 4 wires, and n is 12 to 356 in 8 wires
- EFM mode supports proprietary extended mode for payload rates up to 60Mbps in 8 wires
- Front panel LED indicators for ease of status monitoring
- Standard IEEE 802.1w RSTP for loop prevention and ITU-T G.8032 Ethernet Ring Protection Switch (ERPS)
- Easy installation by DIP-switches, console, Telnet (SSH), WEB GUI (HTTPS), SNMP (v1/v2c/v3) or TR-069
- Remote software upgrade for field-deployed units via TFTP, HTTP or HTTPs
- Ethernet switching, router and bridging with VLAN prioritization and QoS

- Router function supports NAT/NAPT, DNS server/relay, DHCP client/ server/relay, VRRP, RIPv1/RIPv2/BGP/OSPF and static route
- Support security linked feature and TACACS+ authentication for data transmission
- Console/Serial COM switchable, comply with RFC 2217, may connect via TCP client/server or UTP mode

2.2 SHDSL Interface

- Meet ITU-T G.991.2 & ETS TS 101 524
- Bonding protocol: IEEE 802.3ah EFM 2Base-TL
- Support power back off functions
- Modulation Method: 4-TCPAM, 8-TCPAM, 16-TCPAM, 32-TCPAM, 64-TCPAM and 128-TCPAM (4/8/16/32/64/128 levels Trellis Coded Pulse Amplitude Modulation)
- Physical Connection Type: Standard RJ-45 jack, 135Ω balanced via 2 wires, 4 wires or 8 wires twisted pair
- Port enabled / disabled configurable
- Line Protection: meet ITU-T K.21 requirements

2.3 Network Side Interface

2.3.1 Ethernet Interface

- Provide a 10/100 Base-Tx auto sensing and half/full duplex configurable Ethernet Interface
- Physical Connection Type: Standard RJ-45 connector
- Comply with the IEEE 802.3 / IEEE 802.3u
- IEEE 802.3x Flow Control pause packet for Full Duplex in case buffer is full
- Operate as a self-learning bridge specified in the IEEE 802.1d full protocol transparent bridging function
- IEEE 802.1w RSTP for loop prevention
- IEEE 802.1q VLAN Tagging and Q-in-Q, up to 4094 VLAN and VID
- IEEE 802.1p VLAN priority feature by Port-Based of packets for traffic and management

- Up to 2K (2048) MAC learning addresses
- Bridge/Routing application
- Scalable Per Port Bandwidth Control (Step = 64K, up to 100M)
- Ethernet packet length 9K Jumbo frame for LAN and up to 2048 bytes for DSL WAN
- Internal counter/PHY status output for management system
- IPv4 and IPv6
- SNTP (Simple Network Time Protocol) for alarm and event report
- DHCP Client/ Server/ Relay function to automatically get or assign an IP address to a network device
- NAT and NAPT for network address translation
- Point to point PPPoE/ PPTP/ L2TP support
- Virtual IP supports for different VLAN multi-connection
- Different QoS support include 802.1P/ TOS/ DSCP
- Static Routing protocol and dynamic routing protocol include RIPv1/v2, OSPFv2, BGP-4 and Virtual Router Redundancy Protocol (VRRP)
- VPN provides PPTP & L2TP protocol
- Firewall Anti-DDOS attack & ACL security protection
- IEEE G.8032 Ethernet Ring Protection Switch (ERPS)

2.4 OAM

OAM (Operation, Administration and Maintenance) of the Comet 160xF/ FM and 160xF-R/ FM-R Series is listed below:

- Configuration via DIP switches, Telnet (SSH), WEB GUI (HTTP/HTTPS), SNMP v1/v2c/v3 and TR-069
- CID Console: DB9 connector for command line interface (CLI) operation
- TACACS+ (Terminal Access Controller Access Control System) for Authentication, Authorization, and Accounting
- Remote out-of-band control / monitoring via SSH, Telnet and Ethernet
- Remote in-band control/monitoring via G.SHDSL EOC, no IP involved
- Remote Software Upgrade: Remotely via web interface with image file selection; Locally CID console terminal with TFTP protocol

- Configuration backup and restore to / from local profile
- Support hardware or software default configuration setup
- Support Alarm Surveillance function
- Support Performance Monitoring function
- Support three access levels for administrator, operator, user, and operation log
- Support login password complexity of 6 characters, uppercase and lowercase letters, digits, special symbols
- Anti camouflage attack mechanism: lock IP and delay login
- Dying Gasp function indicates the power loss of CPE mode

2.5 Technical Specifications

The following table gives the technical specifications of the G.SHDSL Series.

Table 2-1 Technical Specifications of the G.SHDSL NTU Series

DSL	
Modulation	TC-PAM 4/8/16/32/64/128
Mode	Full duplex with echo cancellation
Number of loops	One subscriber loop on Comet 1602F, 1602F-R Two subscriber loops on Comet 1604F/FM, 1604F-R Four subscriber loops on Comet 1608F/FM, 1608F-R
Loop rate	N*64+8K (N=3~238) up to 15.232Mbps (2 wire), (N=6~576) 30.464Mbps (4 wire), (N=12~1152) 60.928Mbps (8 wire)
Loop impedance	135 ohms
Clock accuracy	± 32 ppm
Interface	
Module	**Ethernet**
	10/100Base-Tx Auto sensing
	IEEE 802.3/ IEEE 802.3u
	IEEE 802.1d full protocol transparent bridging function
	IEEE 802.3x/ 802.1q/ 802.1p/ 802.1ad
	IEEE 802.1w RSTP (Rapid Spanning Tree Protocol)
	Half and full duplex

	Auto cross-over MDI/MDIX detection
	2K MAC learning address
	Ethernet packet size up to 9K bytes
Diagnostics	
LED Indicators	PWR : Power indicator DSL1-4 : DSL status indicator CPE : CPE or CO site indicator LAN1-4 : Ethernet link indicator ALM : Alarm indicator TST : Test status indicator
Craft port	115200bps 8 bits data length, none-parity, 1 stop bit. 9-pin/ D-sub/ female connector, DCE mode
Ser2Net	300~115200bps 5~8-bit data length, Even/ Odd/ None parity, 1 or 2 stop bit 9-pin/D-sub/female connector, DCE mode Protocol: RFC-2217 (Telnet), TCP (Virtual COM), UDP Adaption Mode: Console, Client or Server mode
Ethernet port	LAN port: 10/100Mbps, RJ-45 jack Comet 160xF-R/ FM-R support 4 LAN ports Comet 160xF and 160xFM support 4 LAN ports
Power Requirement	
Input	160xF/ FM: Dual DC: 12V, 36~72VDC AC to DC: 90~240Vac, 40~60Hz Input, 12VDC output Power Input: 4 pin terminal Block*1 (36~72V)/ 12VDC Power Input: 12VDC *2 160xF-R/ FM-R: DC 18-60V, DC 9-36V
Power Consumption	< 7 Watt (160xF/ FM) 8 Watt (160xF-R/ FM-R)

Environments			
Temperature		160xF-R/ FM-R	160xF/ FM
	Operating	0 ~ +75℃	0 ~ +50℃
	Storage	-40 ~ +85℃	-20 ~ +70℃
Humidity	Operating 90% non-condensing Storage 95% non-condensing		

2.6 Applications

This section describes how to apply TAINET Comet 160xF/ FM and 160xF-R/ FM-R Series in the network systems.

2.6.1 EFM Point-to-Point Application

The G.SHDSL Series supports EFM/ATM applications. Figure 2-1 shows the general Point To Point applications using two Comet 1608F or 1608F-R Series. One unit is configured as a central office site (CO) unit and the other is the customer premise equipment (CPE) unit. The EFM scenario as Figure 2-1 can be bridging or routing.

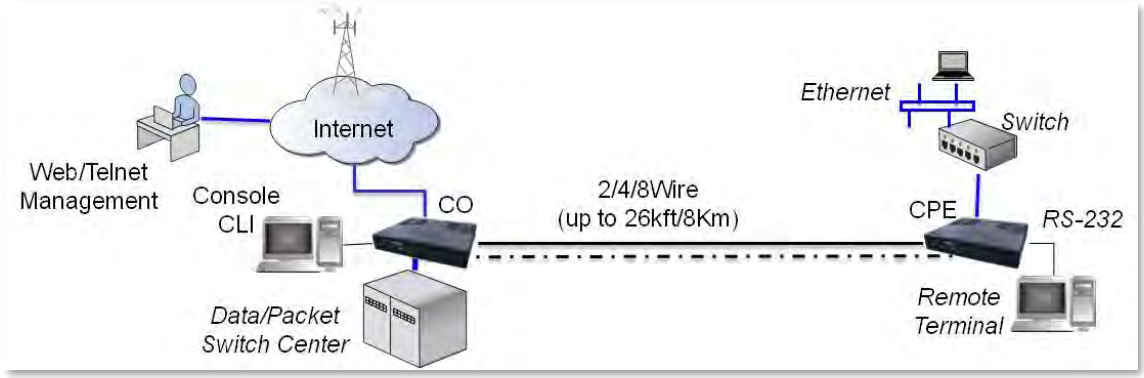


Figure 2-1 P2P Ethernet Application of the Comet 160xF Series

2.6.2 EFM Point-to-Multipoint Application

Figure 2-1 shows the Comet 160xFM supports point to multipoints EFM application. . One unit is configured as a central office site (CO) unit and the other is the customer premise equipment (CPE) unit. The EFM scenario as Figure 2-2 can be bridging or routing.

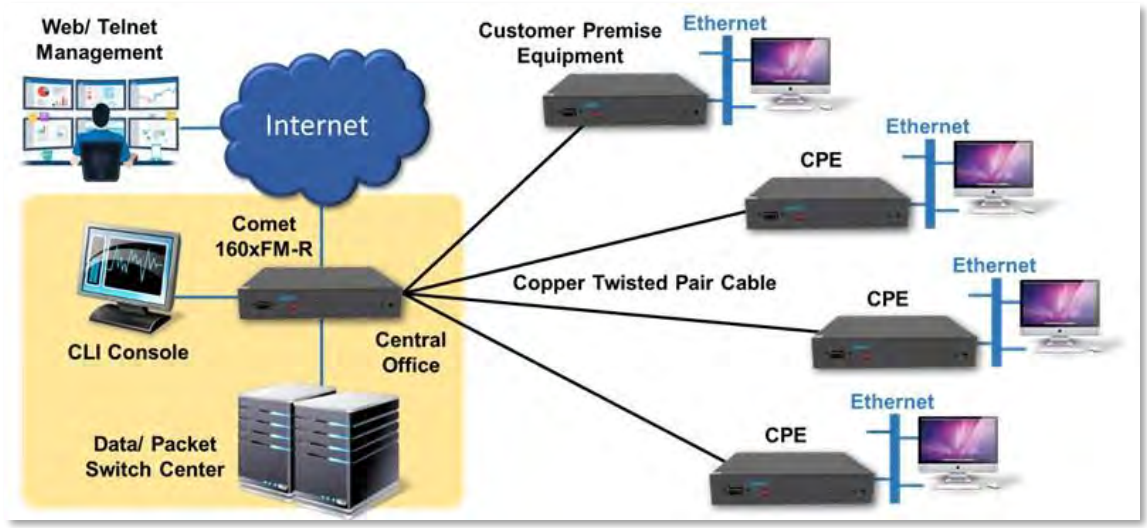


Figure 2-2 P2MP Star Application of the Comet 160xFM Series

2.6.3 Party Line Linear Application

The Comet 160xFM Series supports party line linear application. Figure 2-3 shows the general application by four units. Where multi-mode "MM" is automatic configured as one side is CO, another side is CPE. The DSL trunk can be 2-wire or 4-wire.

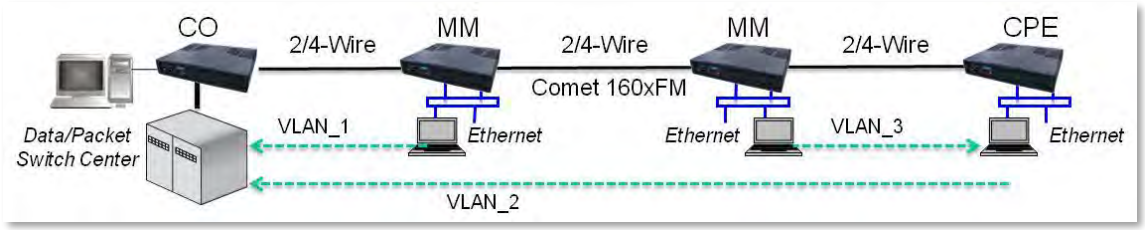


Figure 2-3 Party Line Linear Application of the Comet 160xFM Series

2.6.4 Ring Application

The Comet 160xFM Series supports ring application. Figure 2-4 shows the general application by six units. "MM" is automatic configured as one side is CO, another side is CPE. All DSL trunks connected as a ring network. Select one port of DSL trunk to be subscriber loop protection. This scenario needs to apply the feature of G.8032 or RSTP to avoid subscriber loop errors.

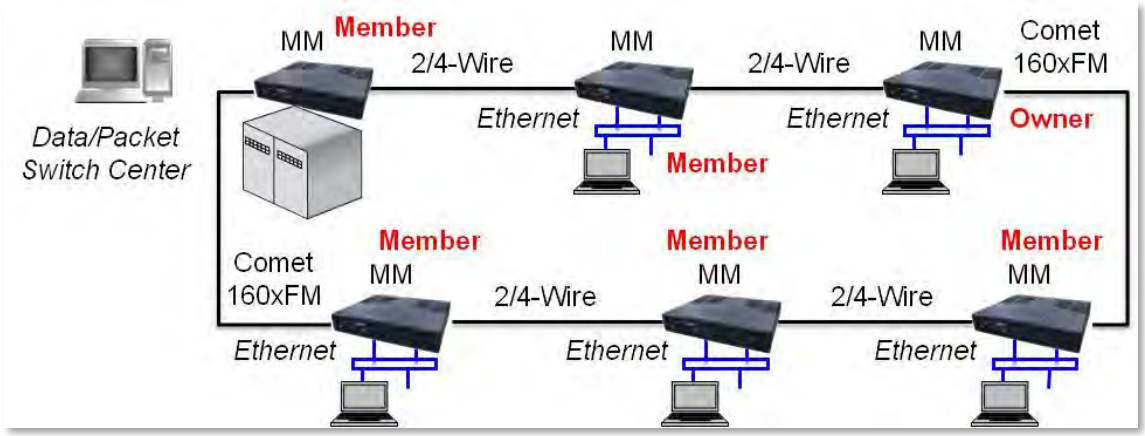


Figure 2-4 Ring Application of the Comet 160xFM Series

Note:

The party line, linear, ring and star topology on G.SHDSL can be used for EFM mode Ethernet traffics on Comet 160xFM models. Other HDLC and ATM mode on G.SHDSL can support to point to point only.

Note:

To apply the Ring application should setup either G.8032 ERPS or RSTP. These two protocols may apply one and only one for the Ethernet traffics loop prevention.

Chapter 3. Interfaces

In this chapter, we will focus our attention on the interfaces of the Comet 160xF/ FM Series and 16xxF-R series. It will show you the front panel & real panel, especially for real panel will be discussed more.

EFM/ ATM models					
Model	G.SHDSL	LAN	G.8032	DIP SW	Craft
Comet 1602F-R	2-wire	4	LAN	●	DB-9
Comet 1604F-R	4-wire	4	LAN	●	DB-9
Comet 1608F-R	8-wire	4	LAN	●	DB-9
Comet 1602F	2-wire	4	LAN	●	DB-9
Comet 1604F	4-wire	4	LAN	●	DB-9
Comet 1608F	8-wire	4	LAN	●	DB-9
EFM only models					
Model	G.SHDSL	LAN	G.8032	DIP SW	Craft
Comet 1604FM	4-wire	4	LAN+DSL	●	DB-9
Comet 1608FM	8-wire	4	LAN+DSL	●	DB-9
Comet 1604FM-R	4-wire	4	LAN+DSL	●	DB-9
Comet 1608FM-R	8-wire	4	LAN+DSL	●	DB-9

Table 3-1 Interface table of Comet 160xF/ FM and 160xF-R/ FM-R series

3.1 Front Panel of Comet160xF/ FM & 160xF-R/ FM-R

The front panel of Comet 160xF/ FM and 160xF-R/ FM-R Series, as illustrated in Figure 3-1, contains four main sections, management port, status indicators, DIP switch and buttons. Via the front panel of Comet 160xF/ FM and 160xF-R/ FM-R Series, users can perform the functions as listed below:

- Displaying system status
- Resetting the device and the alarm LED
- Managing Comet 160xF/ FM and 160xF-R/ FM-R Series via Craft port
- Smart setup by DIP switch
- Test the DSL trunk by TST button

From the status indicators of front panel, users can obtain useful information to monitor the current status.

Figure 3-1 Front Panel of the Comet 160xF/ FM Series

Figure 3-2 Front Panel of the Comet 160xF-R/ FM-R Series

3.1.1 Status Indicators

The status indicators of the Comet 160xF/ FM and 160xF-R/ FM-R are depicted in tables below.

There are six classes of LEDs on Comet 160xF/ FM, which are PWR, TST, CPE, ALM, DSL1-4 and LAN1-4. These LEDs display the system status.

And there are eight classes of LEDs on Comet 160xF-R/ FM-R, which are PWR, TST, CPE, ALM, DSL1-4, LAN1-4. These LEDs display the system status.

Table 3-2 Indicators on Front Panel of Comet 160xF/ FM and 160xF-R/ FM-R series

LED	GREEN	YELLOW	RED	Flashing	OFF
PWR	Power ON				Power OFF
TST		Testing		Testing	No Test
CPE	STU-R				STU-C
ALM			System Alarm	Software upgrade	No Alarm
DSL1-4	DSL Link	Warning	DSL Alarm	DSL handshake	No Used
LAN1-4	Ethernet Link			Ethernet active	Link Down

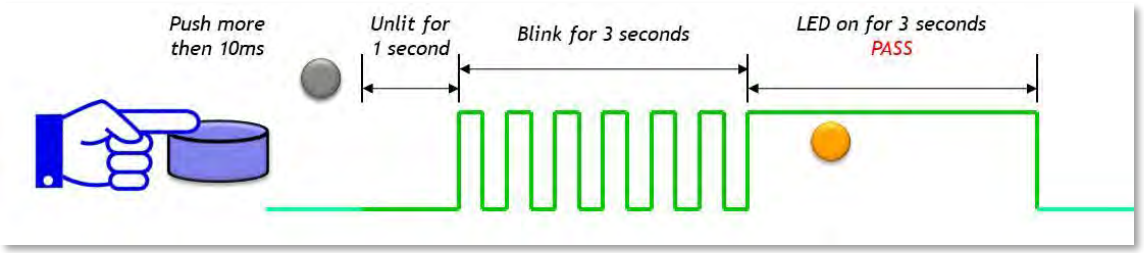
****The front panel indicators on WEB UI may show the 100M full duplex mode of LAN in yellow**

3.1.2 The RST Button

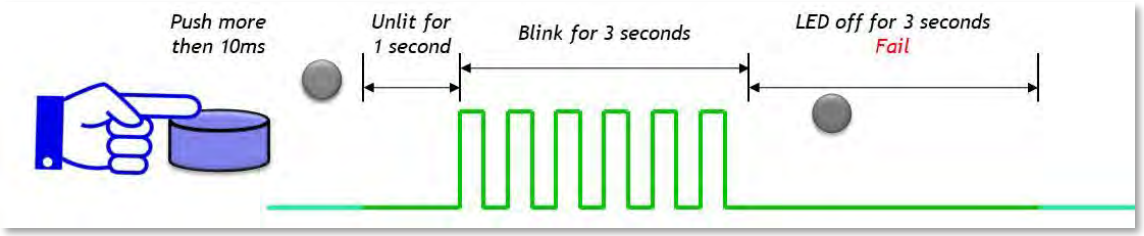
There is one "RST" Reset button to reset the device manually. Push the RST (reset) button for over **5 seconds** will do manually reset the device back to its factory default setting; include login username, password, IP address and all configurations.

3.1.3 The TST Button

This function of TST button is only for the in-service-loop health detection of DSL link between CO and CPE modems. Push the TST (test) button for over 10ms will do loop test, that helps user to test the link status of all subscriber loops.



All loops linked well: if TST LED **keep lighting for 3 seconds** after test. It goes OFF in the first second and then blinks for 3 seconds and finally **light for 3 seconds**.



Any loop links fail: if TST LED **goes OFF after test**. It goes OFF in the first second, then blinks for 3 seconds and finally **keeps dark for 3 seconds**.

3.2 Rear Panel

Figures below illustrate the rear panel of the Comet 16xxF/160xFM Series. Users may connect the Comet Series to other devices or equipment via these interfaces.

Figure 3-3 Rear Panel of Comet 160xF Series (12VDC)

Figure 3-4 Rear Panel of the Comet 160xF Series (48VDC)

Figure 3-5 Rear Panel of the Comet 160xF-R/ FM-R Series

The following connectors/devices appear on the rear panel of the Comet 160xF/ FM and 160xF-R/ FM-R Series.

- Power On/Off: The Comet 16xxF/160xFM Series' power switch
- Power Receptacle: Redundant power for a DC power cable
- Ground line *1
- LAN: Ethernet ports for RJ-45 connector
- DSL Jack: RJ-45 jack for SHDSL link (General or special converter cable)
- DC IN: 12VDC + 36~72VDC or 12VDC + 12VDC (Comet 160xF/ FM)

  9~36VDC or 18~60VDC (160xF-R/ FM-R)

Caution:

Once pressed the "RST" Reset button to reset the device manually, do not lost the power of device during initialing. Otherwise, it will be injured and out of order.

Chapter 4. Installation

In this chapter, we will present the installation guide for Comet 160xF/ FM Series / 160xF-R/ FM-R Series. It begins with a checklist for unpacking the shipping package.

4.1 Unpacking

Comet Series' shipping package includes the following items:

- Comet Series standalone unit
- CE label with User's manual QR Code
- AC to DC Power adapter (for DC 12V models only, the others are option)

4.2 Site Requirements

4.2.1 Site Selection

Install the device in a clean area that is free from environment extremes. Allow at least 6-inch (15.24 cm) in front of the device for access to the front panel, and at least 4-inch (10.2 cm) in back for cable clearance. Position the device so you can easily see the front panel.

4.2.2 AC/DC Electrical Outlet Connection

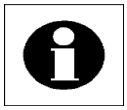
Comet Series with 12VDC input may install within additional AC to DC power adapter be capable of furnishing the required supply voltage, in the standard package of this power adapter can use the AC input range of 100 to 240VAC. With 48VDC input, the DC input range is from 36VDC to 72VDC, the AC input range is from 110VAC to 240VAC at a frequency of 50Hz to 60Hz.

4.2.3 Grounding

Make sure the electric service in your building is properly grounded as described in article 250 of the National Electrical Code (NEC) handbook.

Verify that a good copper wire of the appropriate gauge, as described in Tables 250-94/95 of the NEC Handbook, is permanently connected between the electric service panel in the building and a proper grounding device such as:

- A ground rod buried outside the building at least 8 feet (2.44 meters) deep in the earth.
- Several ground rods, connected together, buried outside the building at least 8 feet (2.44 meters) deep in the earth.
- A wire (see tables 250-94/95 of the NEC handbook for gauge) that surrounds the outside of the building and is buried at least 2.5 feet (0.762 meters) deep in the earth.



Note:

The three grounding devices described above should be firmly placed in the earth. Soil conditions should not be dry where the device is buried.

- If it is unsure whether the electric service in your building is properly grounded, have it examined by your municipal electrical inspector.
- Install a surge protector between the device and Ground point. Any additional computer equipment you have connected to the device (directly or through another device), such as a terminal or printer should also be plugged into the same surge protector. Make sure that the surge protector is properly rated for the devices you have connected to it.
- Call your service provider company and ask them if your leased line is equipped with a circuit surge protector.

If you are operating the device in an area where the risk of electrical surges form lightning is high, disconnect the device from the transmission line at the rear panel when it is not in use.

4.3 Cable Connection

4.3.1 Connecting the IP Network via Ethernet

On the standard unit of Comet 16xxF/160xFM and 160xF-R/ FM-R series, the embedded 10/100Base-T Ethernet port is provided as the standard interface to the TCP/IP network. The pin layout of the RJ-45 connector for IEEE 802.3 standard 10/100Base-T Ethernet ports are defined as following:

Table 4-1 10/100Base-T Connection

Pin #.	Pin Function	Pin #.	Pin Function
1	TD+	5	N/C
2	TD-	6	RD-
3	RD+	7	N/C
4	N/C	8	N/C

For connecting the 10/100Base-T Fast Ethernet, a Category 5 unshielded twisted-pair (CAT.5 UTP) cable or shielded twisted-pair cable is used. Two pairs of the twisted wires are used for separated Rx (reception) and Tx (transmission). The Fast Ethernet port is backward compatible with traditional 10Base-T Ethernet. Comet 160xF/ FM series can automatically detect whether it is connected to a 10Base-T or 100Base-T Network.

4.3.2 Connecting the Terminal

The console port connector labeled "CRAFT" on the front panel of Comet 160xF/ FM and 160xF-R/ FM-R is provided for connection to an external ANSI or VT-100 compatible terminal to do local configuration of Comet 160xF/ FM and 160xF-R/ FM-R. Craft port Speed & Data format: 115,200bps, no parity, 8 data bits, 1 stop bit, and no flow control.

Craft port define in DB9 connector

DB9	Pin 1	Pin 2	Pin 3	Pin 4	Pin 5	Pin 6	Pin 7	Pin 8	Pin 9
	N/C	RXD(o)	TXD(i)	N/C	GND	N/C	RTS(i)	CTS(o)	N/C

Table 4-2 Table Craft Port defile in DB9 connector

4.3.3 Connecting the DSL on Devices

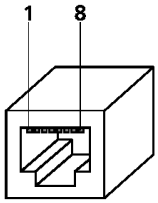
Comet 160xF/ FM and 160xF-R/ FM-R provide 2, 4 or 8 wires connection on DSL port.

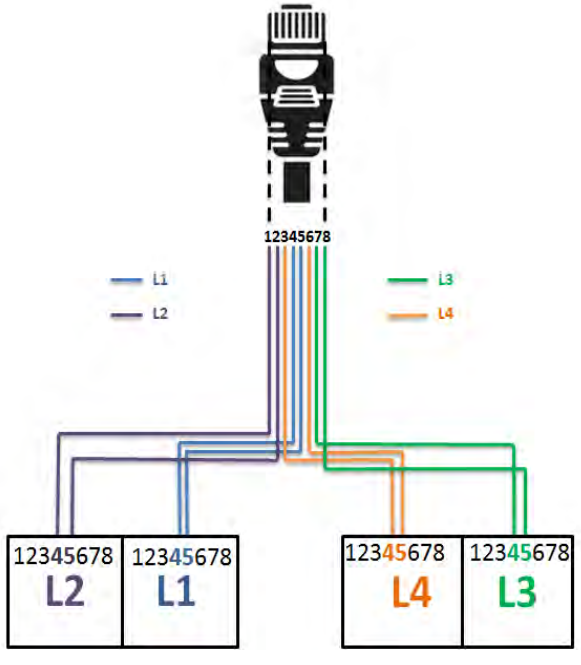
Figure 4-1 Comet 160xF/ FM Series DSL Interface

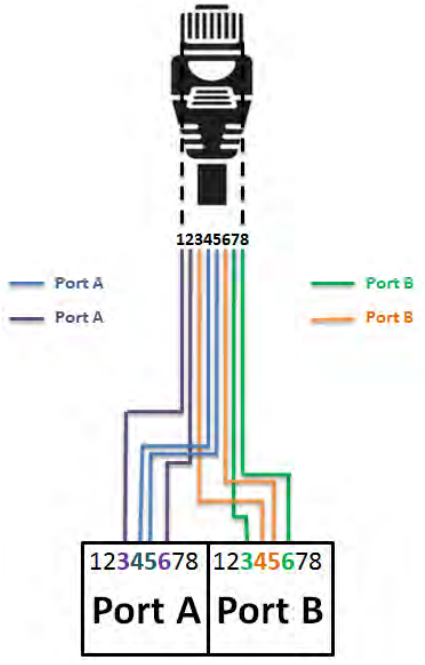
The DSL interface used the RJ-45 connector for 1, 2 or 4 pairs of DSL to connect, with the pin configuration as shown in the Appendix A.3 and table below. Whereas the mix mode connection of Comet 1608FM or 1604FM may apply the different connector for Port A(CPE) and Port B(CO) mode connection in one box.

Table 4-3 DSL Twisted Pair Pin Assignment

Pin	2W	4W	8W	PortA	PortB
1			Tip(2)		
2			Ring(2)		
3		Tip(2)	Tip(4)	Tip(2)	Tip(3)
4	Tip(1)	Tip(1)	Tip(1)	Tip(1)	Tip(4)
5	Ring(1)	Ring(1)	Ring(1)	Ring(1)	Ring(4)
6		Ring(2)	Ring(4)	Ring(2)	Ring(3)
7			Tip(3)		
8			Ring(3)		







4.4 Quick Setup

Comet 160xF/ FM and 160xF-R/ FM-R Series have "DIP Switch" on the front panel for quick setup. It provides users to quickly configure the device to CO (Central Office) and CPE (Customer Premises Equipment) to the other modem.

Figure 4-2 Comet 160xF/ FM Series DIP Switch

- Keep local DIP switches to all **OFF** (Default CPE mode).
- Change the remote unit **DIP-1** switch to **ON** (As a CO mode).
- Connect the DSL loops as the PIN defined.
- Connect the DC power jack and feed the power to start working.

Caution:

When turned the **DIP-2** to **ON,** the Ser2Net function may take place the console privilege to control. Do remember to keep a static IP address for WEB management, in case of either Console or Ser2Net one to be used.

Note:
When turned the **DIP-2** to **ON** and then **OFF**, the Ser2Net function will be disabled, and the craft port can back to console control.

Chapter 5. Operation of Web

In this chapter, user will be introduced to the WEB operation of Comet 160xF/ FM Series. The chapter starts with an overview of device' WEB. In additional, each main menu item of WEB interface, such as Configuration, Maintenance and Status will be explained thoroughly. The following introductions are based on the Comet 16xxF with firmware code **v1.430**.

5.1 Overview

Firstly, users have to connect to the LAN port, which is the default management port, and enter the IP address as the URL in the Internet browser. The default IP address of management is http://192.168.0.1.

Comet 160xF/ FM and 160xF-R/ FM-R Series support the following WEB browsers:

1. Microsoft Edge 109+
2. FireFox 80+
3. Safari 10+
4. Google Chrome 80+

5.2 Login Page

In this page, users need to enter the correct name & password. There are three built-in accounts with different privileges.

- Administrator - username: **admin**, password: **admin**
- Operator (user) - username: **user**, password: **user**
- Monitoring (guest) - username: **guest**, password: **guest**

Figure 5-1 Login Page

Please use the following pull down menu option to select displayed language.

Figure 5-2 Language selection

5.3 Status

Local & Remote status can be obtained in this section. Besides, Comet 160xFM supports only local settings, without remote function, due to improve the stability in its point to multipoint ability.

5.3.1 Local/ Remote Status

For 8-wire model, there are four subscriber loop indexes: DSL1, DSL2, DSL3 and DSL4. Thus, DSL1 and DSL2 are available for 4-wire mode, and DSL1 is only available for 2-wire mode.

The following information is showing Line Status, Current Alarm and Current Performance.

Note: For 8-wire model (Comet 1608F), the total speed is the summary of all loops' Line Rate.

For instance, if all loops are at full speed (89 x 64kbps = 5696kbps), the total speed of DSL trunk is 4 x 5696 = 22784kbps.

The first view of Status windows is "**Current Alarm**" that shows the following information: Loop/Port/LAN, Name/Type and Severity.

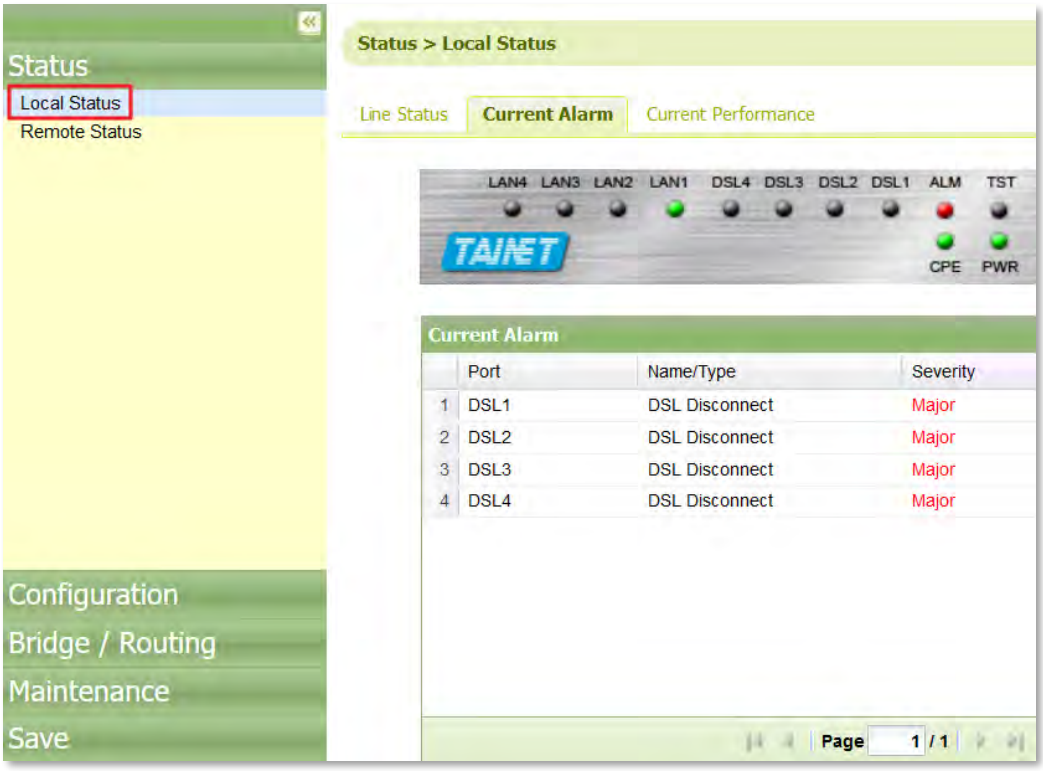


Figure 5-3 Current Alarm

The following interface status will show in "**Line Status**":

- **G.SHDSL Status:** shows the following information: Loop Index, Line Rate, Line Status, TC-PAM, SNR (Signal Noise Ratio) and ATTN. Users can also check the current mode (EFM/ ATM) and total line rate in this form for different models.
- **Ethernet Status:** shows the following information: LAN Index, LAN Speed, LAN Status and Flow Control.

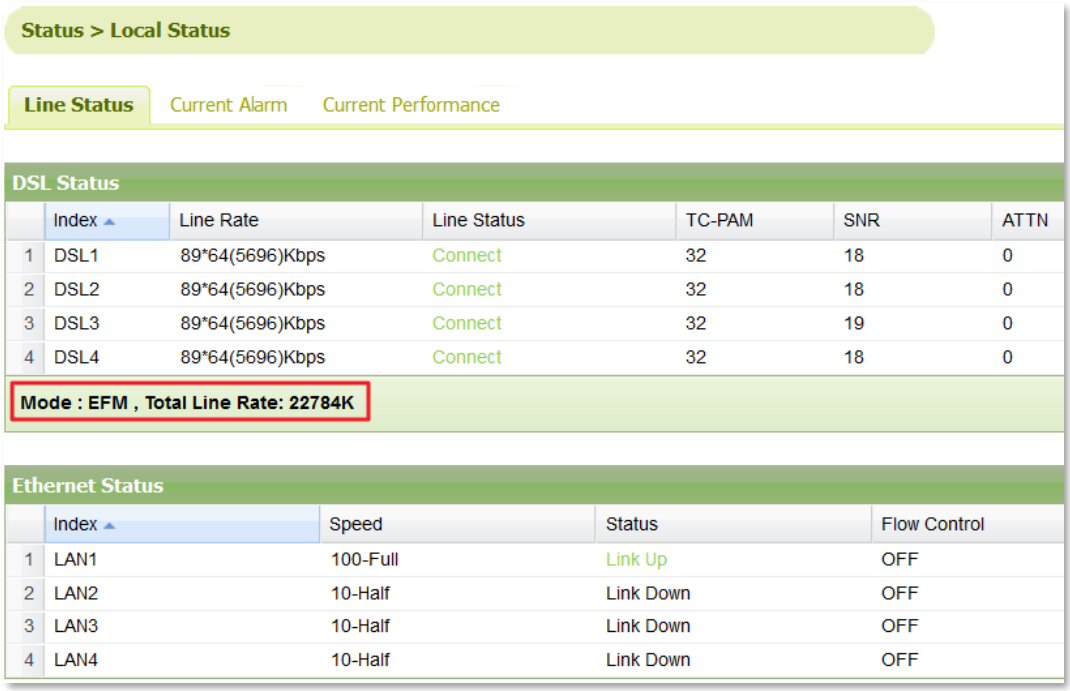


Figure 5-4 Line Status

- **Current Performance:** shows the current performance error of G.SHDSL in 15 minutes and 1 Day duration.

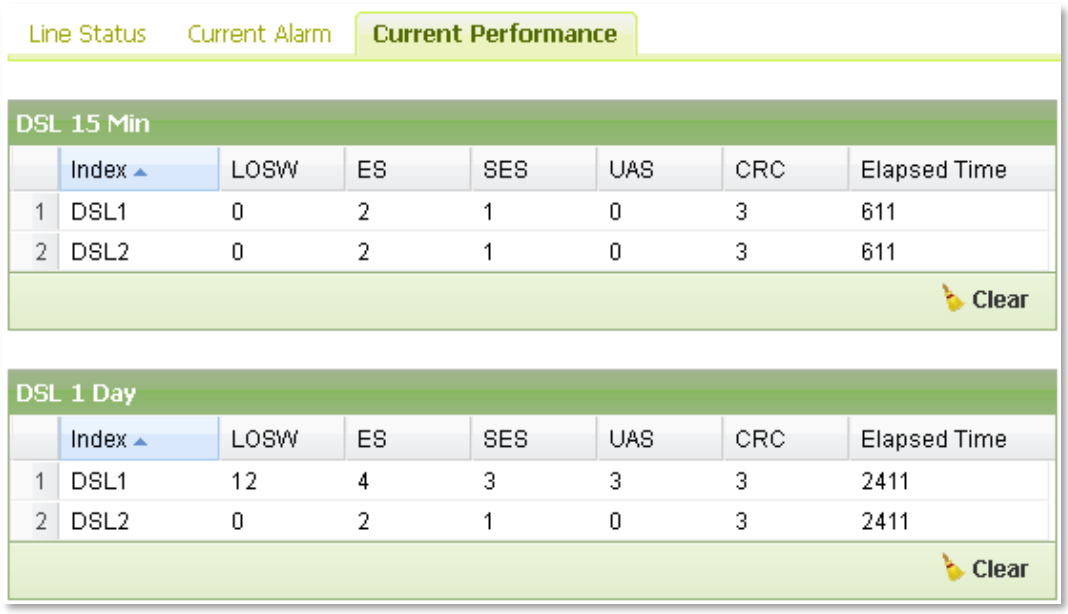


Figure 5-5 Comet 160xF/ FM Current Performance

- **LOSW:** Lost of Sync Word seconds.
- **ES:** Error Seconds
- **SES:** Severely Error Seconds
- **UAS:** Unavailable Seconds

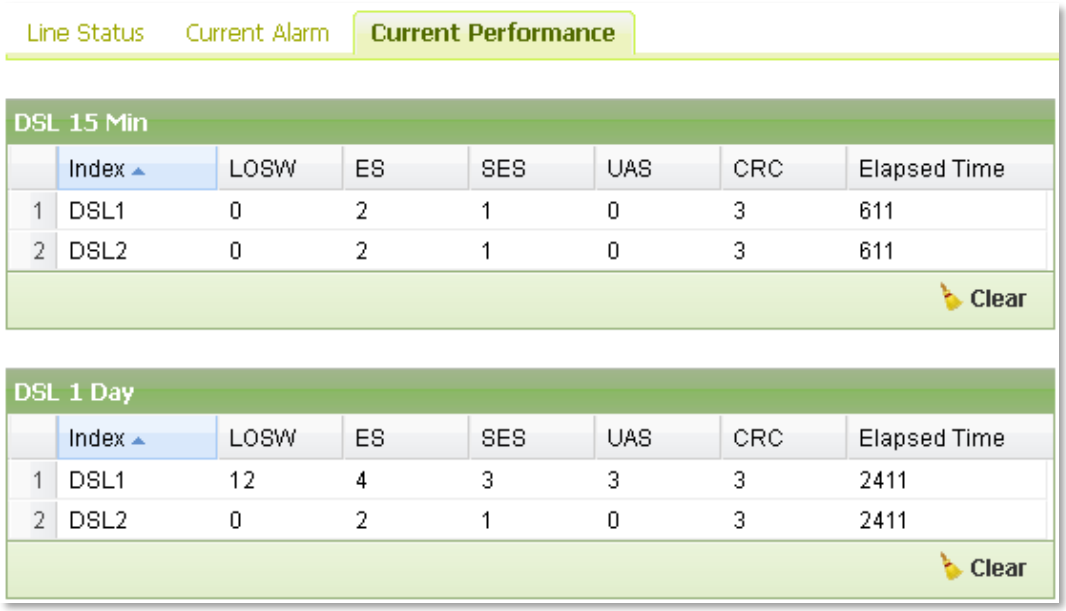


Figure 5-6 Comet 160xF/ FM Current Performance

5.4 Configuration

Comet 160xF and 160xF-R/ FM-R Series support Local/Remote configuration except of Comet 160xFM have only local available due to improve the stability in its point to multipoint ability.

5.4.1 Load Local Profile (Remote Profile)

There are two default profiles in Comet 160xF/ FM and 160xF-R/ FM-R for users to select, as shown in Figure below, the default profile is CPE mode. If a pair of DSL lines is applied to field, users can select local one to CO mode (profile 1) and another one to CPE mode (profile 2) for quick setup.

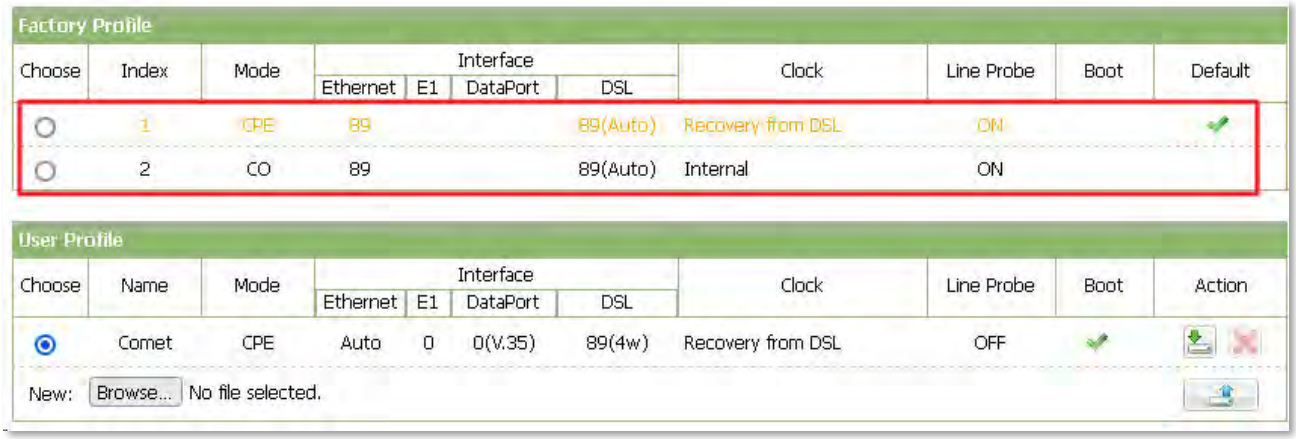


Figure 5-7 SHDSL Load Local/Remote Profile

The operator may save and restore their "User Profile" for keeping all modified configuration. And for the quickly deployed to other devices, these "User Profile" can be saved and restored in local storage as a file mode for ease of backup.

5.4.2 Local Setting (Remote Setting)

There are three modes being selected by users: EFM, HDLC & ATM

- **EFM mode:** Users can modify the parameters of G.SHDSL and Ethernet. The clock source is selected automatically. And there is a proprietary extended mode for up to 15.232Mbps per pair in G.SHDSL connection.
  Note: Comet 160xFM supports EFM mode only
- **HDLC mode:** Users can only modify the parameters of G.SHDSL and Ethernet. The default clock of G.SHDSL is 3a, user can setup the clock 1 via CLI mode. In HDLC, there is no extended mode for upmost speed.
- **ATM mode:** Users can modify the parameters of G.SHDSL, Ethernet & ATM. In ATM form, General Setup includes basic ATM protocols and ATM Parameters for VID, VPI and VCI. (Comet 160xFM does not support ATM mode)

Figure 5-8 Local/Remote Setting in Different Mode

5.4.2.1 G.SHDSL Setting in EFM mode

- **Topology setting:** Only Comet 160xFM has topology setting function, for doing ring, star or linear topology. This feature supports five modes below. If users would like to do linear or star topology, it can be selected to "p-to-mp". And if ring topology is needed, it can also be selected to "mixed mode", which has to be set with G.8032 (Ring Protection feature).

Topology setting	Description
point to point (Default)	Disable the topology function.
p-to-mp (4W/8W<->n*2W)	One device has only one master-slave mode, which connects to other four devices by 8-wire.
mixed mode (8W<->2*4W)	One device has two modes (CO & CPE) with 8-wire.
mixed mode (4W<->2*2W)	One device has two modes (CO & CPE) with 4-wire.
p-to-mp (8W<->2*4W)	One device has one master-slave mode with 8-wire. The setting can be configured on CO side only.

Table 5-1 Topology setting table

- **DSL Isolation:** Default is "**Disable**", all pairs in point to multipoint mode will be bounded together, lead all data packets spread through each of DSL sections. As it is "**Enable**", all remote devices except of central one will not negotiate with each other because of all data packets in DSL are separated.

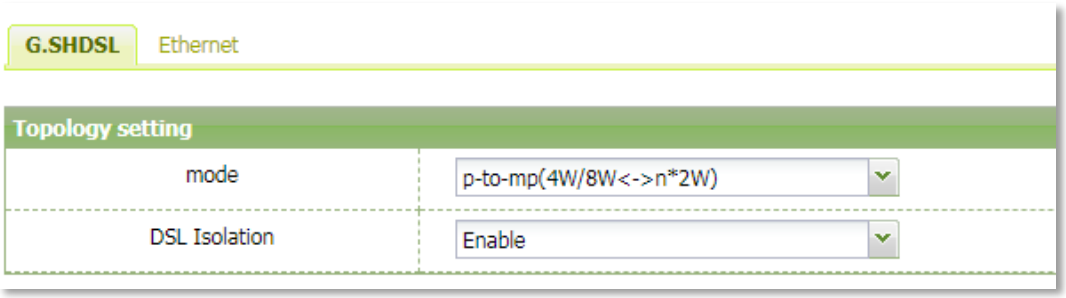


Figure 5-9 Topology setting

- **G.SHDSL configuration:** Some items of function can be done by STU-C in CO mode only, for example, "**Line Rate**" and "**Power Backoff**" are not allowed to configure in **CPE**.
- **Wire Mode**: Comet 160xF Series support 2W, 4W, 8W and Auto.
- **Power Back off**, PBO Value:

  Power back off used to reduce the data transmission power for the duration of loop connection. When it set to "Auto", Comet dynamically reduces the power level in order to eliminate the potential for interference with the digital local loop resulting from near-end crosstalk. There is only STU-C in CO mode can change the setting of "Power Back off". As soon as it set to "Manual", then "PBO value" (Power Back off value) can be filled from 0 to 31 dB attenuation.

- **Line Probe:**

  When it set to ON, the device adjusts the DSL line data rate automatically according to line quality of SNR (Signal Noise Ratio) Margin, the higher the SNR value, the better the DSL line quality. When SNR value is very low, the DSL line might become disconnected.

- **Annex:** Users can select A/F suitable for North American networks or B/G suitable for European networks connecting DSL.

- **Capability List:** New capability can use for proprietary extended mode. While old capability is compatible with legacy SHDSL connection.
- **Auto Sensing (EFM/ ATM)**: This can work during DSL handshaking to decide with remote EFM or ATM mode.
- **Target Margin:**

  If the actual SNR value is lower than SNR margin value, the device will decrease the line rate to prevent SNR value from dropping and keep the DSL link to up. However, users should be aware of that there is a relationship between the line rate and connection distance. When the DSL line rate goes higher, the DSL line connection distance becomes shorter and vice versa.

- **Extended Mode:** In EFM mode, the standard ITU-T G.991.2 supports TC-PAM4/ 8/ 16/ 32 modes. While Comet support proprietary TC-PAM64/128 mode to reach more date rate. TC-PAM 128 would be up to 238 x 64Kbps.
- **Miscellaneous:** For Comet 160xF/ FM, 160xF-R/ FM-R Series, the setting is fixed. CO side is "**Internal**", and CPE side is "**Recovery from DSL**".
- **Threshold**: For better troubleshooting, users can choose the threshold of ATTN, SNR and CRC, in order to generate alarm traps report.

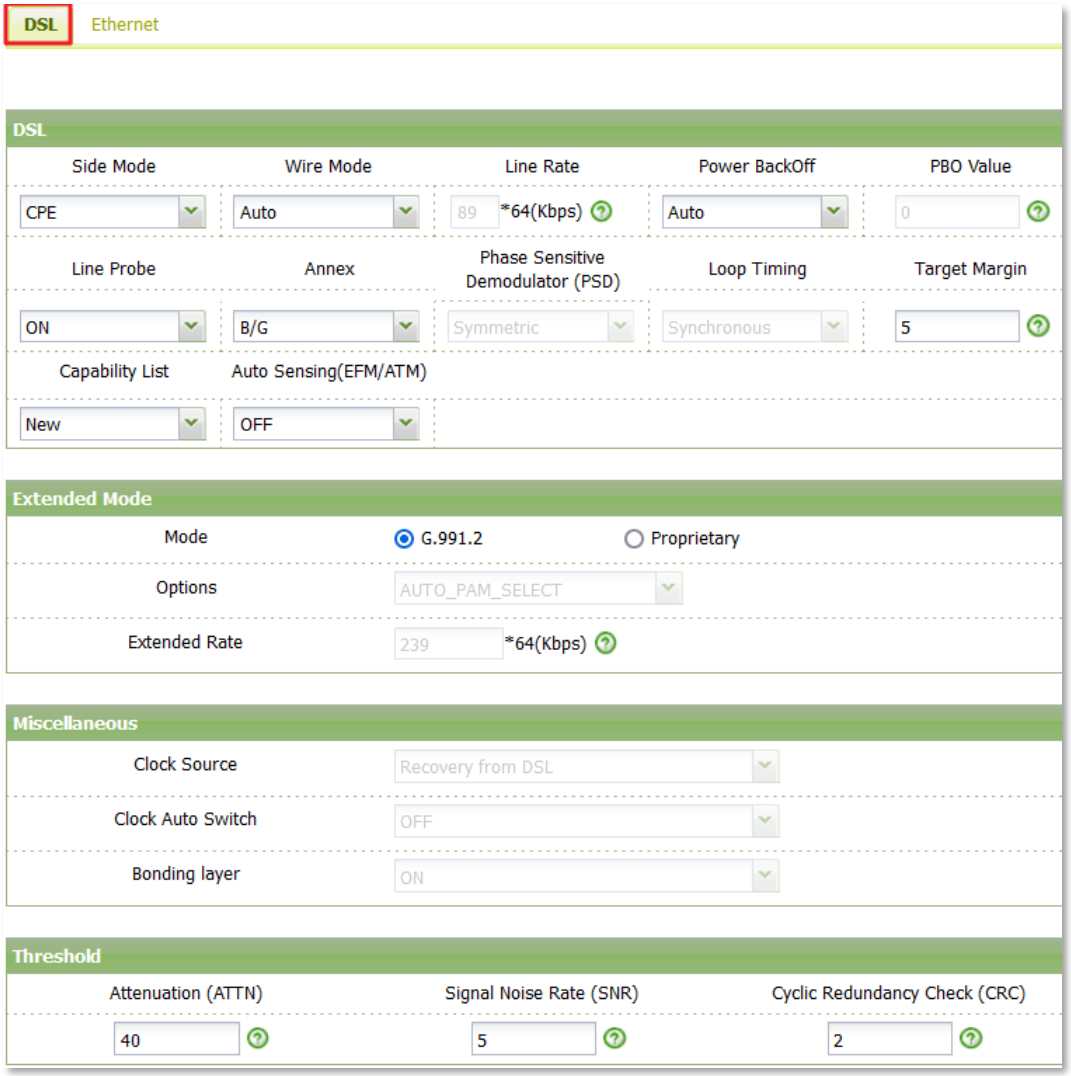


Figure 5-10 Local/Remote Setting in G.SHDSL

5.4.2.2 Ethernet Setting

Except TDM mode, users can configure relative Ethernet parameters in the form, such as Admin, Speed, Alarm Switch, Flow Control, Ingress and Egress.

- **Admin:** The LAN port will be turned off if users configure it to be "**OFF**".
- **Speed:** The default speed is "Auto", users can select 10-Half, 10-Full, 100-Halt or 100-Full.
- **Alarm Switch:** If users turned the "**Alarm Switch**" on, then alarm message will be reported during Ethernet interface got problems.
- **Flow Control:** The default Flow Control is "**ON**", users can select "**OFF**" to disable.
- **Ingress:** There is no Ingress limitation in default condition. Users can define the input traffic as 64Kbps to 50Mbps.
- **Egress:** There is no Egress limitation in default condition. Users can define the input traffic as 64Kbps to 50Mbps.

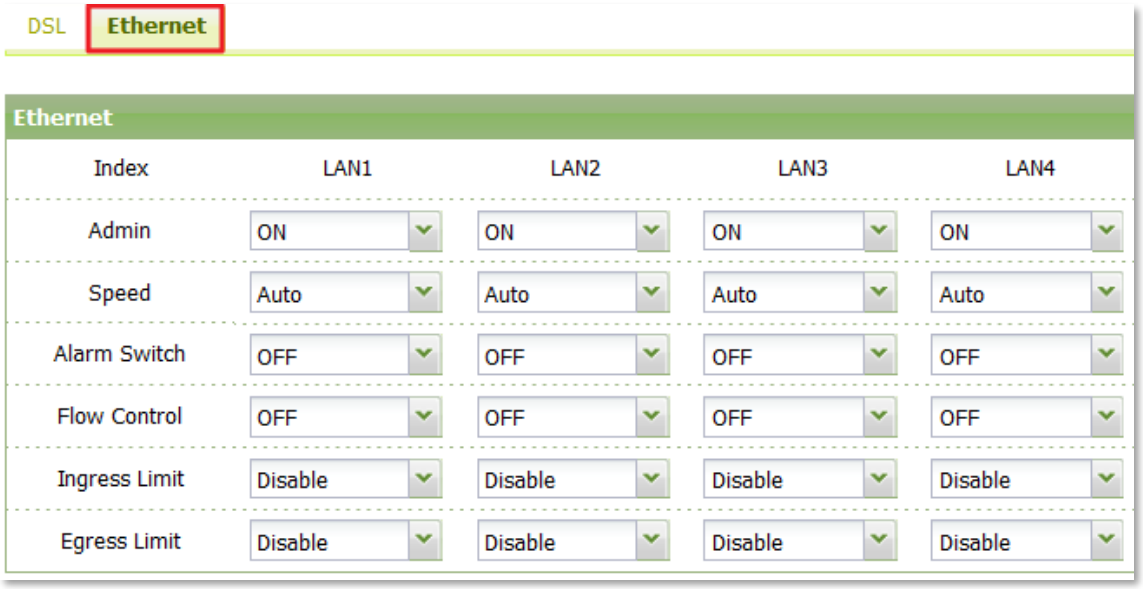


Figure 5-11 Local/Remote setting in Ethernet

5.4.2.3 ATM Settings in ATM mode

There are two main forms in ATM: **General Configure** and **ATM Parameters**.

- General Configure

CPCS Protocol: CPCS is "Common Part Convergence Sub-layer". Header is to identify the protocol that Virtual Circuit is carrying. LLC_ENCAP_BP is "Logical Link Control Multiplexing, and VC_MUX_BP is "VC-based Multiplexing".

Filter Mode: The setting is VLAN ID, for multi-PVC and rules.

Default Action: The default action is "**Default VPI/VCI**". As long as the packets mismatch with VLAN ID, the rule will do Default VPI & VCI. If the default action is "**Discard**", devices will drop the packets with mismatched VLAN ID.

Default VPI/VCI: VPI is "**0**", and VCI is "**35**".

- ATM Parameters

There are eight Virtual Path Identifiers in the ATM table.

VID: The limitation of VLAN PVID is from 1 to 4095.

VPI: The limitation of Virtual Path Identifier is from 0 to 255.

VCI: The limitation of Virtual Channel Identifier is from 32 to 4096.

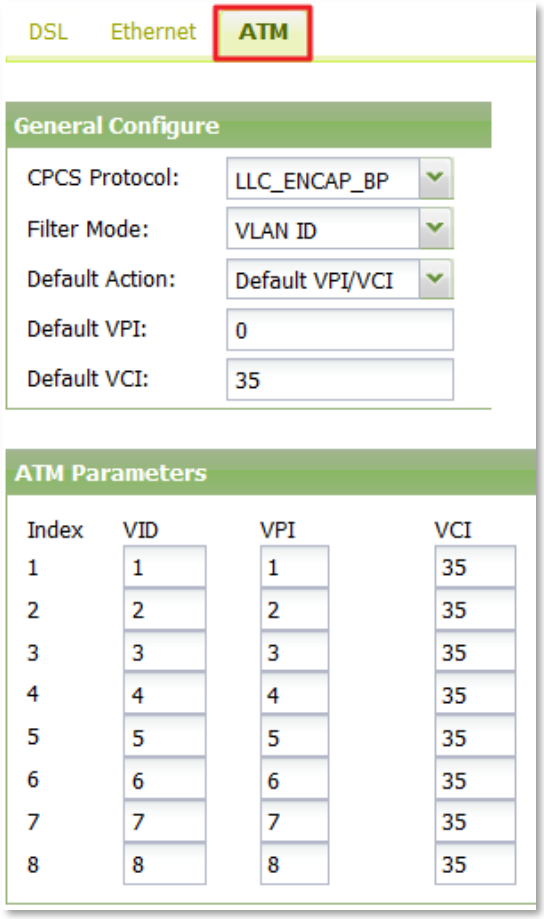


Figure 5-12 Local/Remote setting in ATM

5.4.3 User Management

In this page, there are three built-in privileges for different users' deployment. To improve the security level, remember to follow the security mechanism while creating new accounts.

- Administrator – has highest operation privilege to control all function, it can add, delete or modify all accounts.
- Operator - has highest operation privilege to control all function, except to create either delete any accounts.
- Monitor - has limited operation privilege to read information only.

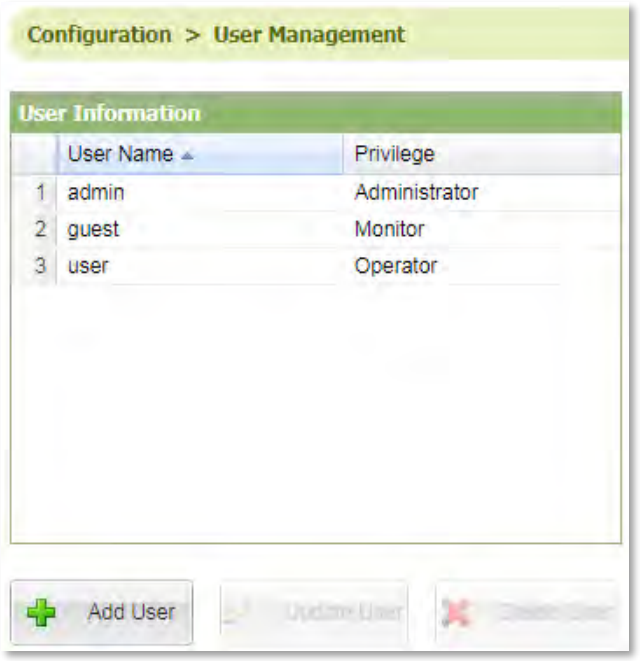


Figure 5-13 User Management

5.4.4 TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) improves on TACACS functions of Authentication, Authorization and Accounting by encrypting all traffic between the NAS and the daemon. It is extensible to provide for site customization and future development features, and it uses TCP to ensure reliable delivery. The protocol allows the TACACS+ client to request every fine-grained access control and allows the daemon to respond to each component of that request.

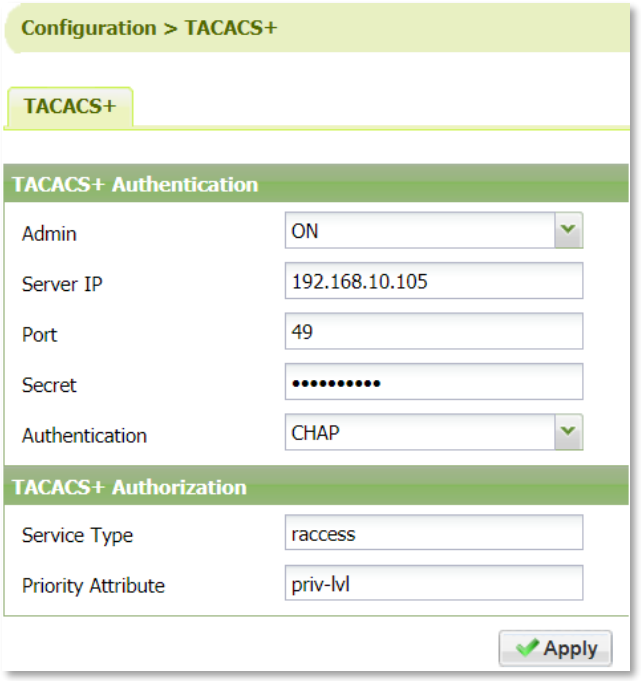


Figure 5-14 TACACS+ setup

- **Admin**: The default parameter is "OFF", switch it to "On" to start the TACACS+ authentication.
- **Server IP**: The IP address of TACACS+ server located.
- **Port:** The default TCP port of TACACS+ is 49.
- **Secret**: The phrase string for using as authentication key.
- **Authentication:** The phrase string to be authentication type of ASCII, PAP or CHAP.
- **Service Type:** For making authorization call by service type of arap, shell, ppp, slip, vpdn or raccess.
- **Priority Attribute:** The Attribute Value (AV) pairs parameter for priority, they are text strings exchanged between the client and server.

5.4.5 Date & Time (Local/Remote)

SNTP (Simple Network Time Protocol) is a protocol that synchronizes the clock of local devices, as client, to exactly match the clock at the central server system. Accurate time information is critical for monitoring the device with system log.

The device supports two ways to be configured, one is communicating with SNTP server for retrieving the time, another is the time can be set manually. And the [Daylight saving time] function may enable the clock to move one hour early.

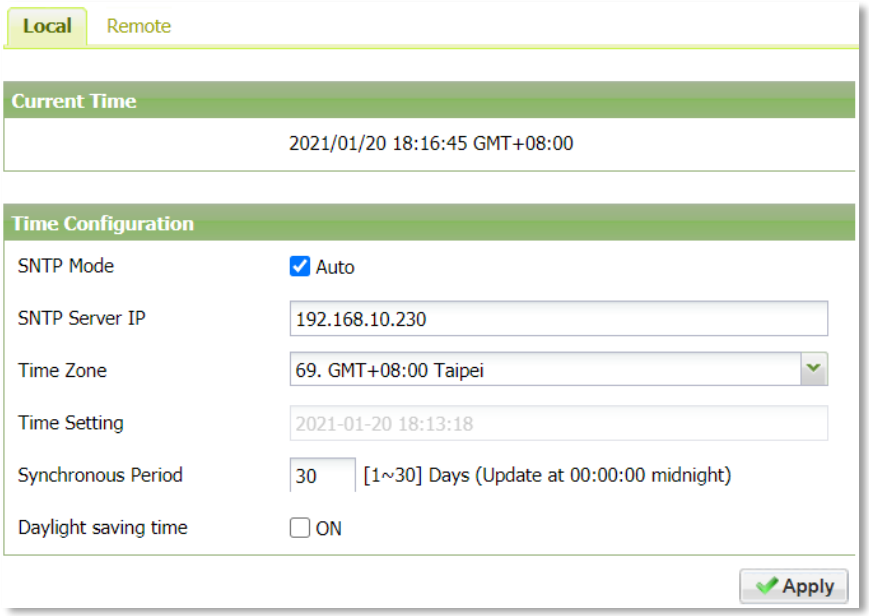


Figure 5-15 Local/ Remote Date & Time

5.4.6 General Setup (Local/ Remote)

IP configuration can be configured only in this menu within **Bridge** application. The menu includes two main items, "**System IP**" and "**Link Security**".

System IP: It is the IP address of this device for management. The system IP may

change immediately after operator clicks the apply button, but this change will not save the new IP address before next power on. Remember to save after configured.

Link Security: The link security function asks for input 6 fixed digital numbers (0-9). While the security link function is enabled on CO, the system will keep checking the link password between CO and CPE side. If the security passwords are not the same, the system will disconnect the DSL link and try to build up the DSL link to check the security password again.

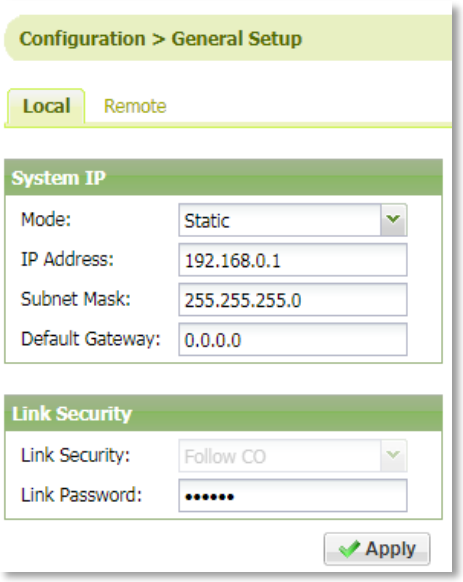


Figure 5-16 Local/ Remote General Setup

Note:

The IP Address assignment of "System IP" may switch to "Virtual IP" in Bridge/ Routing menu if the "Bridge VLAN Setting" changed its VLAN rule from **port based VLAN** to **Tag-based** or **Q-in-Q**.

5.4.7 DHCP Server

- **Configuration**: Users can change the DHCP mode from OFF to DHCP server or DHCP relay (Resolve that server & client need to be in the same network). If operators configured the SHDSL modem as DHCP server, most important settings are "**Start IP**" and "**End IP**", should be the same network segment as device's LAN. Other requirements, such as "**Lease time**", "**Gateway**", "**NTP Server**" or "**DNS IP**" would be followed to operators' environment.

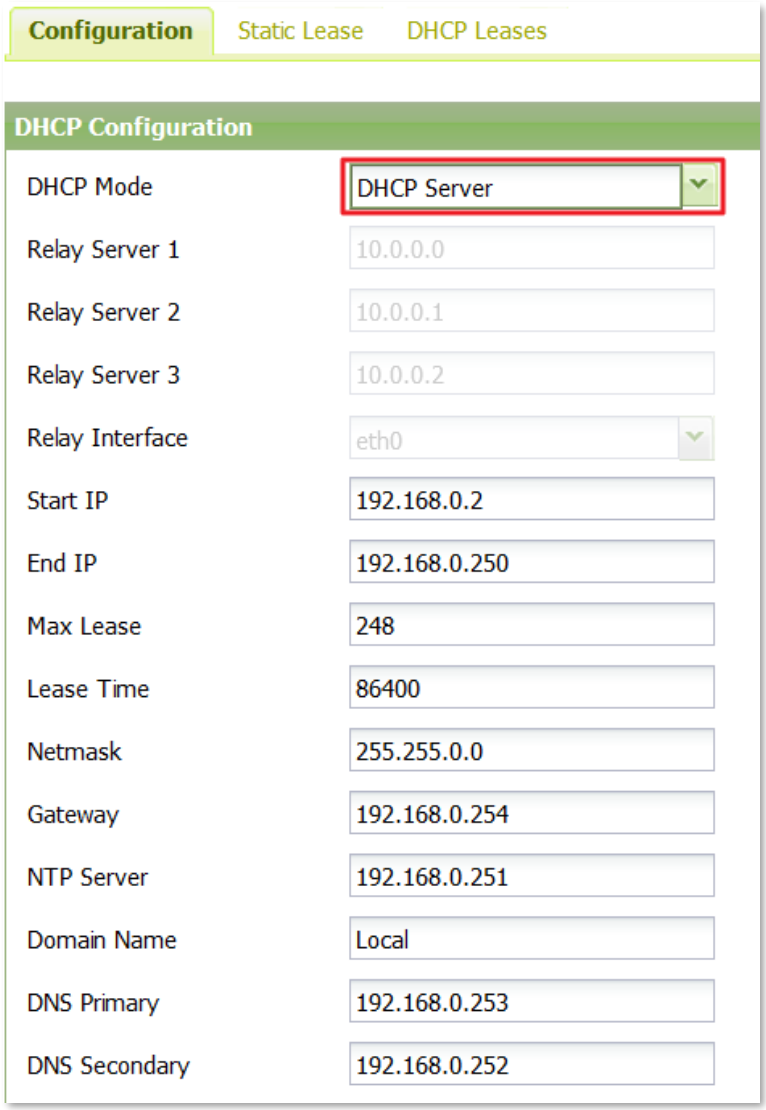


Figure 5-17 DHCP Server Configuration

- **Static Lease:** The function is work with DHCP server, operators assign a specified IP to a specified DHCP client, the way of identification is to check DHCP client via MAC address. Users also have to make sure the specified IP is working between "**Start IP**" and "**End IP**".
- **DHCP Leases:** The window includes IP, MAC address and Expire time. When the SHDSL modem acts as a DHCP server, device will record all DHCP clients.

5.4.8 IPv6 (Local/Remote)

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol. IPv6 was developed by the IETF to deal with the long-anticipated problem of IPv4 address exhaustion. Comet 16xxF/ 160xFM and SNTU 76xF series follow the future trends and multi-application. The IPv6 packets can pass through DSL, and also manage the device via IPv6. Users can configure the "**Admin**", "**Link Security**", "**IP Address**", "**Prefix**" and "**Default Route**".

- **Admin:** The default parameter is "**Disable**", switch it to "Enable" to open the IPv6.
- **IP Address:** It is the IPv6 address of this device for management, the setting would change immediately after operators click the "**Apply**" button, but this change will not save the new IPv6 address for next power on. Operators must to click "**SAVE**" to save IPv6 address. The format of this item is

  "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx"

  After click the "Apply" button, users will access the device by inputting **[IPv6]** in the browser.
- **Prefix:** Prefix lengths of IPv6 identify a range of IP address those are in the same network. The default prefix length is "**64**".
- **Default Route:** Users can accept the device to access to other networks via default route.

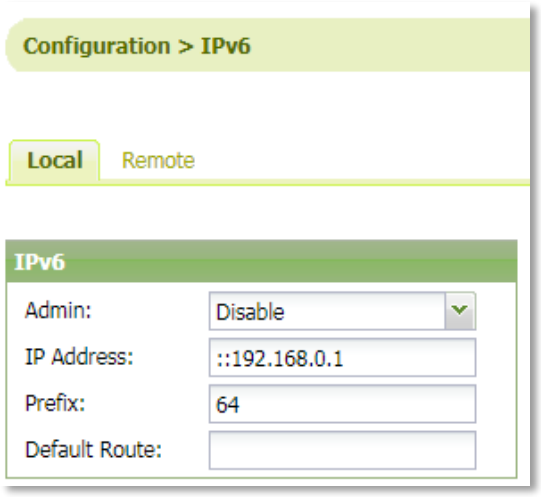


Figure 5-18 Local/Remote IPv6

5.4.9 SNMP & SysLog

To set up the trap IP of the system, users can go to the Trap submenu. Input and activate the desired IP address / Domain name. The setting value must be effective by pressing "Apply" button. When the trap or syslog IP is configured, the G.SHDSL device alarm information will send to these destination addresses. The trap IP address is usually the address of the SNMP network management system.

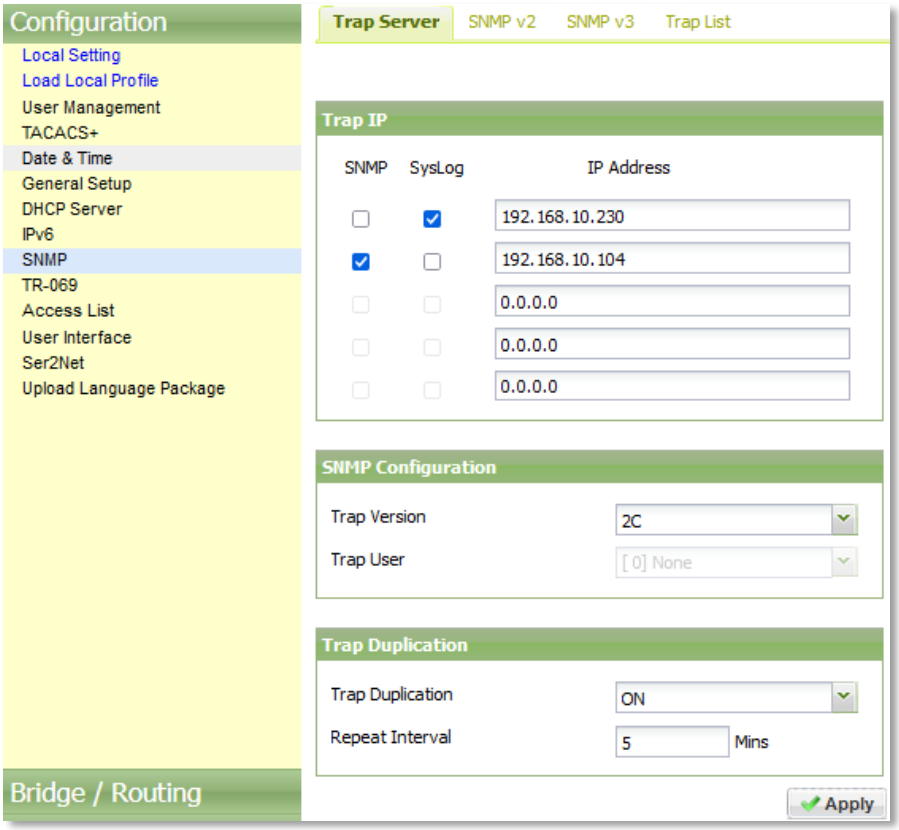


Figure 5-19 SNMP Trap Server

Set agent public and private keys in SNMPv2. The default Public Community key is "public" and Private Community key is "private".

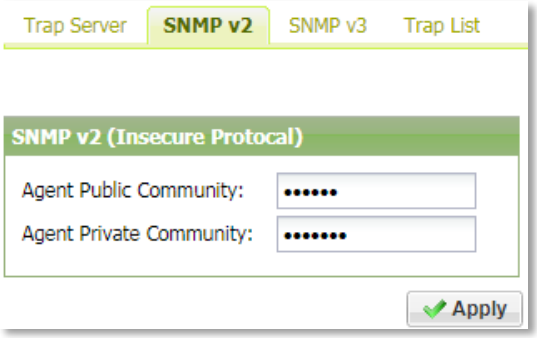


Figure 5-20 SNMP v2 Setup

To set up the security level of SNMPv3, we recommend users configure the permission to Auth & Priv, it is much safer. In other items, SHA is safer than MD5, and AES is safer than DES.

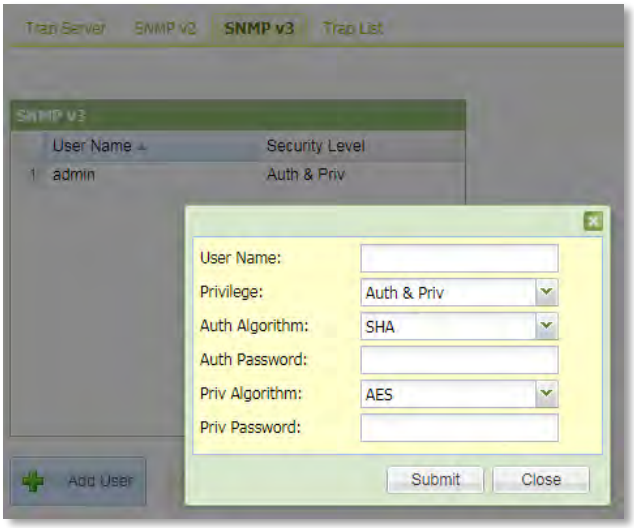


Figure 5-21 SNMP v3 Setup

Users can change the severity in the trap list. There are critical, major, minor and warning being selected. Remember to click the "**Apply**" button after configured.

Trap List

Code	Name	Severity	Cause
2	Data Port Service Alarm	Major	Data port loss of signal.
3	G.SHDSL Link Service Alarm	Major	G.SHDSL line disconnect.
4	G.SHDSL Signal Attenuation Alarm	Minor	G.SHDSL Line Signal Attenuation exceed Threshold.
5	G.SHDSL SNR Alarm	Minor	G.SHDSL Line SNR exceed Threshold.
6	G.SHDSL CRC Alarm	Minor	G.SHDSL Line CRC exceed Threshold.
8	DSL Pin Assignment Reversal Alarm	Auto	DSL twisted pair pin assigment reversal.
9	Remote Powered Off	Major	Remote powered off.
10	Lan Service Alarm	Major	Lan link down.
11	E1 LOS Alarm	Major	E1 Loss Of Signal.
12	E1 LOF Alarm	Major	E1 Loss Of Frame.
13	E1 AIS Alarm	Major	E1 Alarm Indication Signal.
14	E1 RAI Alarm	Minor	E1 Remote Alarm Indication.
15	Sys Clock Auto Switch	Major	System Clock Auto Switching.
16	No Trap Events	Clear	No Trap Events.

Figure 5-22 Trap List

5.4.10 TR-069

Comet 16xxF/ 160xFM support TR-069 protocol, which acts as ACS client, all parameters in this form are designed to communicate with ACS server. In order to pass the ACS certification successfully, be sure to check all parameters are consistent with each ACS server and client. For instance, input the entire "**ACS URL**"

as *http://IP:Server Port/*, input the "**CPE port**" as port number and so on.

- **Mode:** Default parameter is "**Disable**", and the "**Enable**" is to run the TR-069.
- **CPE Port:** ACS client port number.
- **Connection Request User Name**: Define Comet's user name, the device has its own authentication, to let ACS server access.
- Connection Request Password: Define Comet's password.
- **ACS URL**: The way to access ACS server is using URL.
- **Login ACS User Name**: Refer to ACS server's user name.
- **Login ACS Password**: Refer to ACS server's password.
- **Periodic Inform**: Comet 160xF/ FM will request ACS server to keep communicating at regular intervals.
- **Periodic Interval**: The unit of time is second.

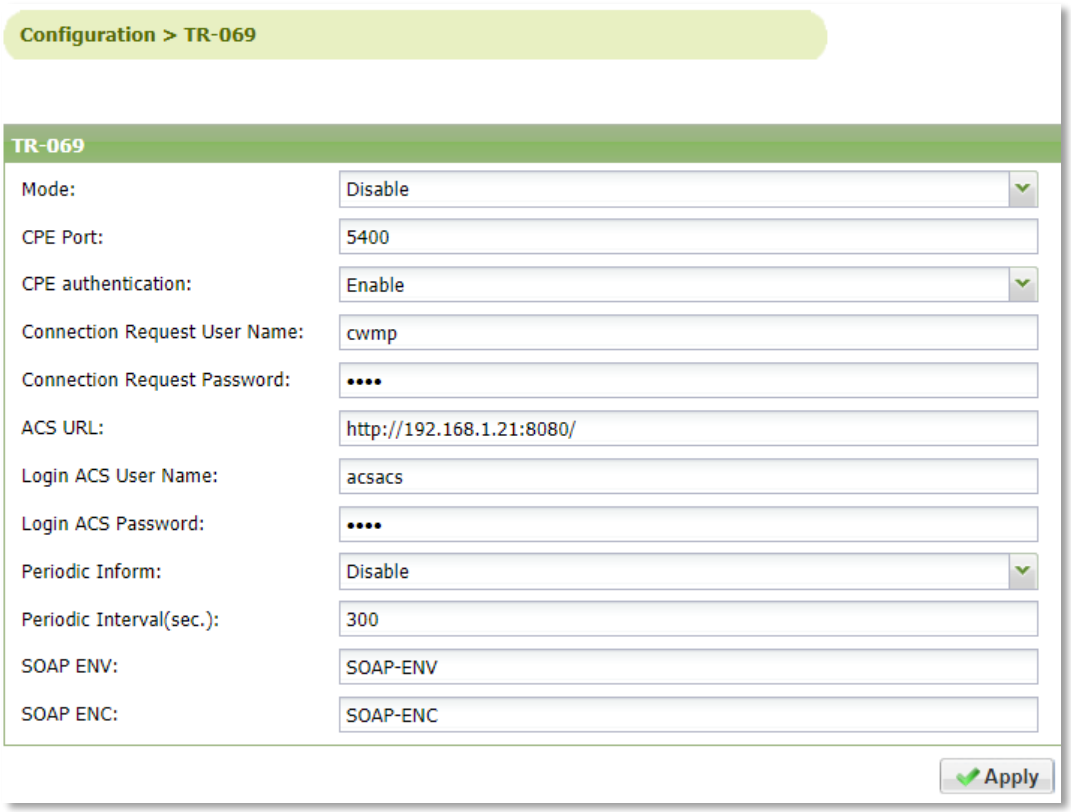


Figure 5-23 The TR-069 parameters

5.4.11 Access List

In order to filter data packages, Comet 16xxF/160xFM needs to set a series of rules for identifying what need to be filtered. The device supports ACL "**White List**" mode and "**Normal**" mode.

- **White List:** All data need to match one of all rules could pass through the devices, otherwise, any mismatch ones will be dropped.
- **Normal:** All data need to exactly match all rules will be dropped or forwarded to

specified physical ports.

Matched conditions of ACL rules can be MAC, ETH Type, IP address and TCP/ UDP port number. An ACL rule may contain one or several sub-rules, which have different matched conditions.

- **Frame Type:** Select ACL type, "**MAC**" or "**IPv4**".
- **Action:** There are two behaviors, "**drop**" or "**forward**".
- **Physical Port (Ingress):** Select ingress port to do ACL function.
- **Physical Port (Egress):** Select egress port to do ACL function.
- **ETH Type:** Table 5-2 list some EtherType example for reference

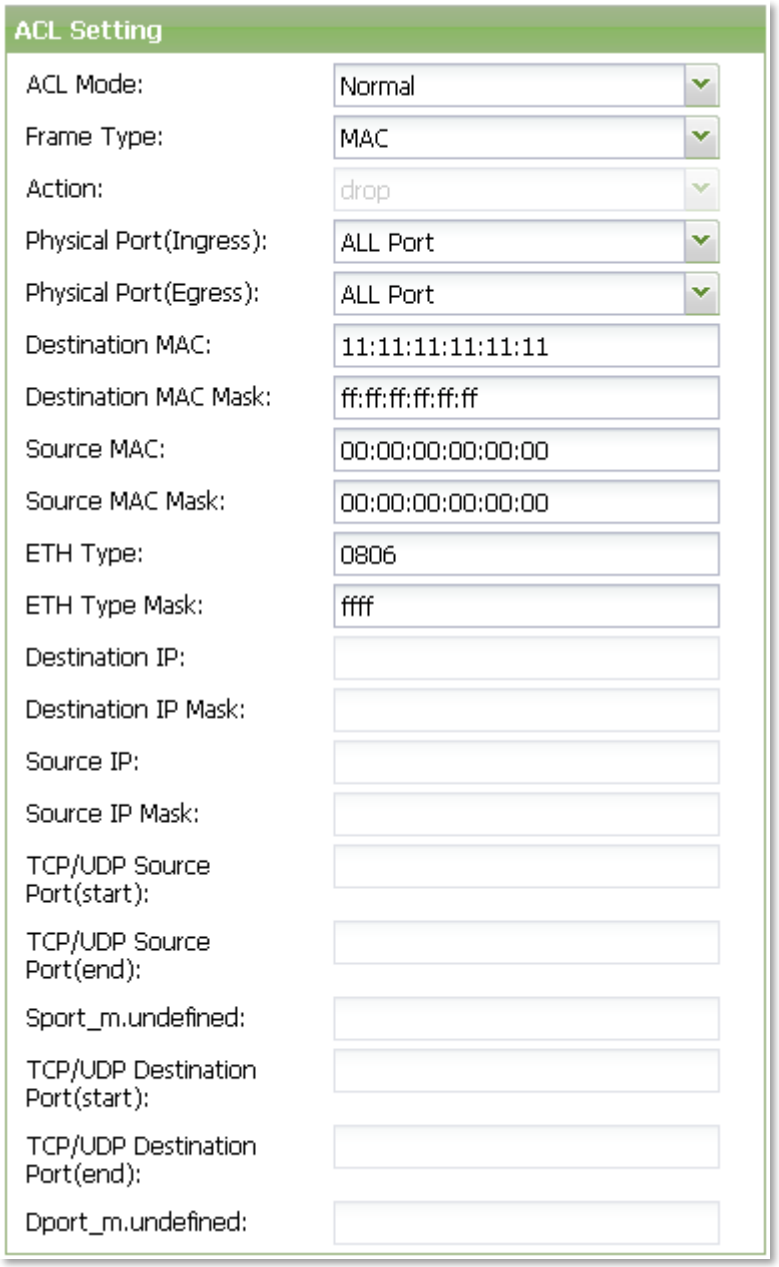


Figure 5-24 ACL Setting

Before click "Apply" to take effect ACL setting, please make sure whether the rules will make the WEB management loss or not. After click "Apply" button, users can check the rules in "**Show ACL Table**".

Figure 5-25 Show ACL Table

Table 5-2 The Example of EtherType

EtherType	Protocol
0800	Internet Protocol version 4 (IPv4)
0806	Address Resolution Protocol (ARP)
0842	Wake-on-LAN[9]
8035	Reverse Address Resolution Protocol (RARP)
809B	AppleTalk (Ethertalk)
80F3	AppleTalk Address Resolution Protocol (AARP)
8100	VLAN-tagged frame (IEEE 802.1Q)
86DD	Internet Protocol Version 6 (IPv6)
8808	Ethernet flow control
8847	MPLS unicast
8848	MPLS multicast
8863	PPPoE Discovery Stage
8864	PPPoE Session Stage
88A4	EtherCAT Protocol
88A8	Service VLAN tag identifier (S-Tag) on Q-in-Q tunnel.
88CC	Link Layer Discovery Protocol (LLDP)
88F7	Precision Time Protocol over IEEE 802.3 Ethernet
9100	VLAN-tagged (IEEE 802.1Q) frame with double tagging

5.4.12 User Interface (Local/Remote)

Users can enable or disable different network service port in Comet 160xF/ FM and 160xF-R/ FM-R Series, there are Telnet, SSH, HTTP, HTTPS, and account protection.

- **Account Protection:** A common threat on web login is a password-guessing attack. The account protection is a way to temporary block brute-force attacks about 5 minutes that simply lock out accounts after 3 times of incorrect password attempts.
- **Management IP/Mask:** "Permit" means without limited for any IP address. And "Limited" will allow only which PC located in specified in Management IP/Mask.

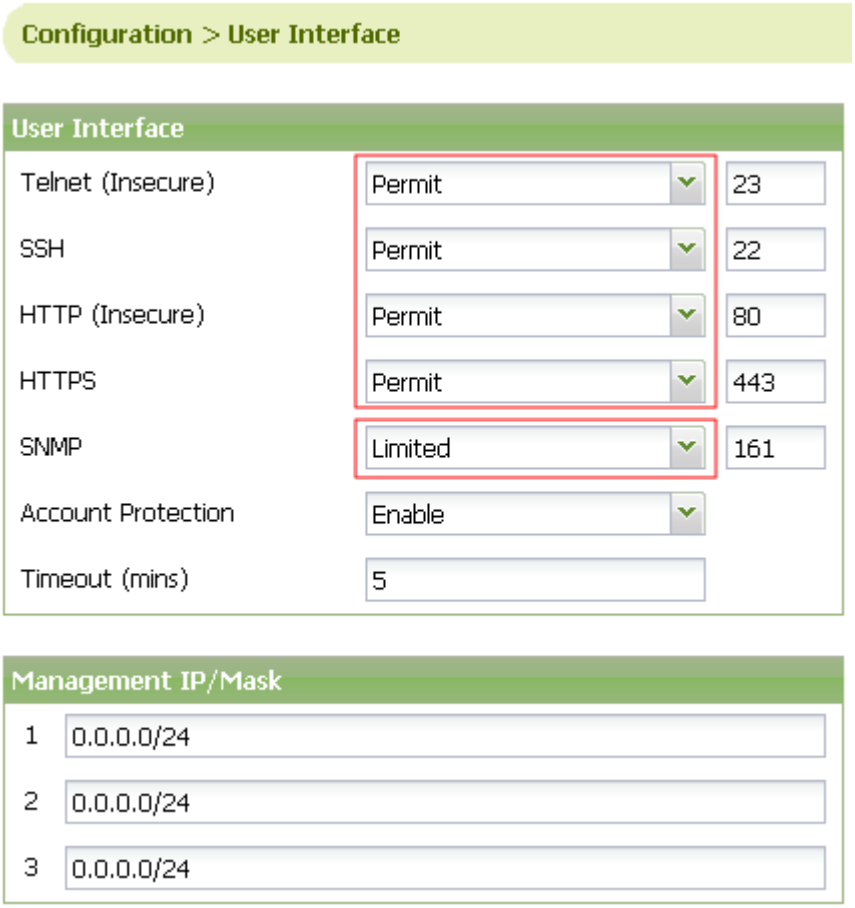


Figure 5-26 Local/ Remote User Interface

5.4.13 Ser2Net

Repackage RS-232 data as IP formats then transmit to network is one kind of smart solution for industrial center. Not only pass RS-232 data through network, but also could manage remote device by RS-232 interface.

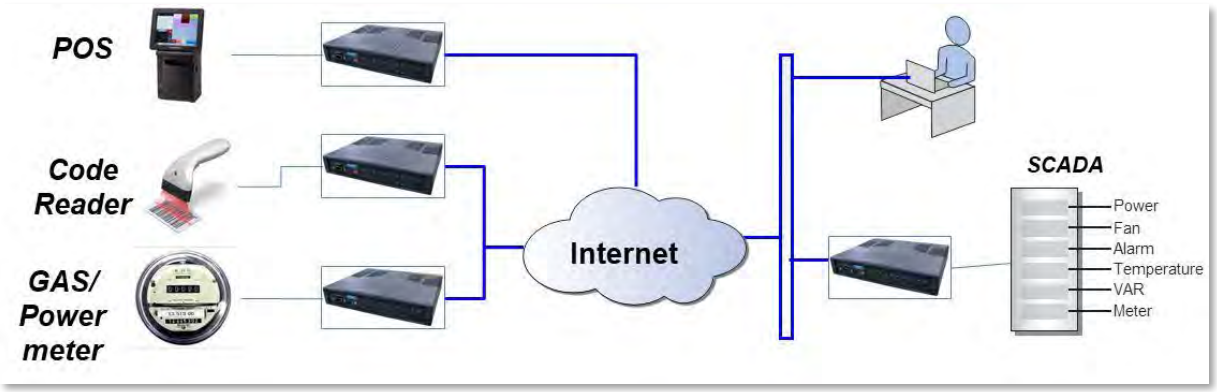


Figure 5-27 Serial port to IP application

- **Admin** – Turn **ON** or turn **OFF** the serial port to IP function.

Caution:

When turned the **Admin** to **ON,** the Ser2Net function may take place the console privilege to control. Do remember to use a static IP address for WEB management, in case of either Console or Ser2Net one to be used.

- **Link Type** – There are Telnet, TCP and UDP mode selection. The Telnet and TCP type can choose Server or Client mode of the Serial port as a virtual console that connects with remote device. And the UDP type can work for one to four (4) remote devices in broadcast mode.
- **Mode** – Act as Server or Client mode for Telnet and TCP link.
- **Port** – TCP/IP, UDP port number.
- **Remote IP 1~4** – Client & Server pair, the UDP mode may play one to four remote devices.
- **Idle Timeout (s)** – Disconnect the link session if exceed the timer.
- **Baud Rate (bps)** – The serial port data speed, may select from 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200bps.
- **Data Bit** – The length of data bit in asynchronous frame of Serial transmission, may select from 5, 6, 7 or 8 bits.
- **Parity Bit** – The type of parity check in asynchronous frame of Serial transmission, may select from None, Even or Odd types.
- **Stop Bit –** The length of stop bit in asynchronous frame of Serial transmission, may select in one (1) or two (2) stop bits.

Note:

The console port of Comet series acts as RS-232 DCE mode for data communication. It can use straight RS-232 cable connect to PC Terminal (DTE mode) or use with additional null modem connect to other DCE devices.

Figure 5-28 Convert serial port to IP Network

5.4.14 Upload Language Package

Comet 160xF/ FM and 160xF-R/ FM-R Series support to upload a local language file to replace original English menu tree. That will help international user to operate it easily. For the sample form of this local language file, please contact with local distributor or TAINET support by E-MAIL: sales@TAINET.net

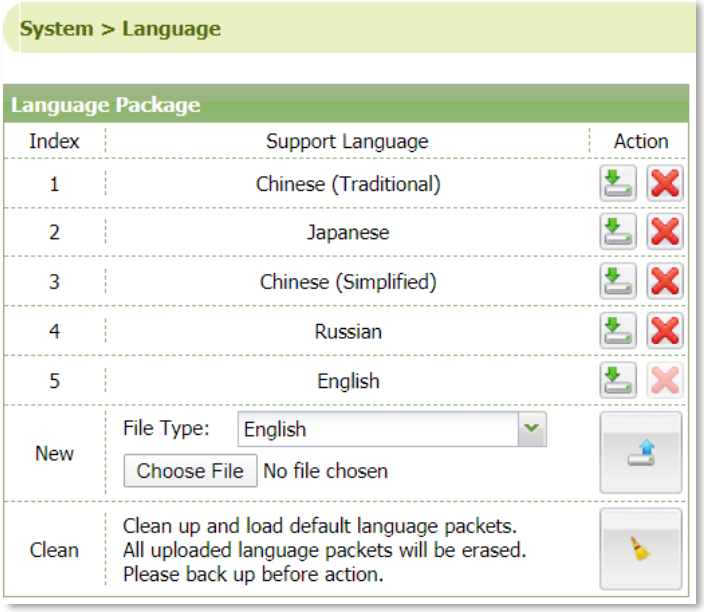


Figure 5-29 Upload Language Package

5.5 Bridge / Routing

5.5.1 General

There are two main windows in this menu, "**QoS Setup**" and "**Aging-Time**". To quantitatively measure quality of network service, several related aspects of the network service are often considered, such as packet loss, bit rate and transmission delay. Comet 160xF/ FM and 160xF-R/ FM-R Series could provide different priority to different applications, or to guarantee a certain level of performance to a data flow on different ports.

- **Type:** Port Priority (Default), TOS/DSCP and 802.1p
  - **TOS/ DSCP:** According to 802.1Q TOS (Type Of Service) and DSCP (Differentiated Services Code Point) to distinguish the Ethernet frame priority
  - **802.1P:** The enhanced QoS of 802.1Q, with additional PCP (Priority code point) from 0 to 7 priority level. 7 is the highest priority and 0 is the lowest priority.
- **Schedule:** WRR (Weighted Round Robin) and Strict Priority
- **Aging-Time**: The default aging-time for MAC address learning is 300 seconds; users can configure it for saturated release time.

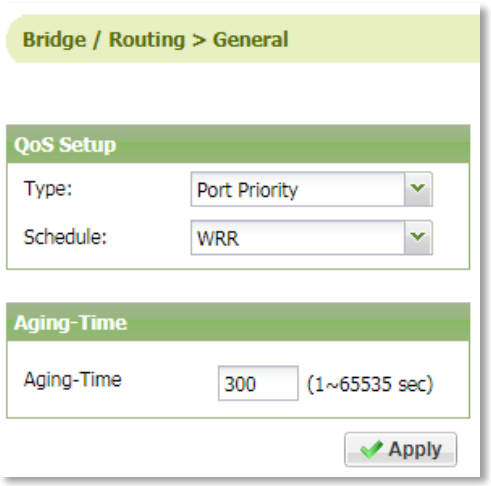


Figure 5-30 QoS Setup

5.5.2 VLAN

There are three rules of VLAN available on Comet 160xF/ FM and 160xF-R/ FM-R Series, "**Port-based**", "**Tag based**" and "**Q-in-Q**". Default parameter is "Port-based" for passing through all kinds of traffics. For further management, switch VLAN rule to "Tag-based" is the first step to enable basic VLAN and VLAN translation.

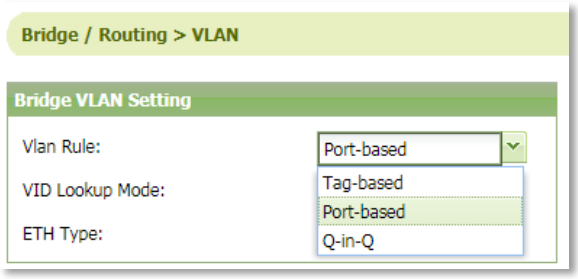


Figure 5-31 VLAN Rule

The Ethernet switch can use VLAN information to select the ports among which traffic can be forwarded. Based on IEEE 802.1Q, the VLAN table is used to handle traffic in accordance with user-defined forwarding rules, up to 4094 VLAN rules. The user can configure it on each LAN port, whether it will participate in Tag VLAN. Port-based VLAN has been already configured in default.

- Port-based VLAN

Port-based VLAN is a logical group of ports. The function has been already configured and users will be unable to define the Ethernet switch. Traffic within the VLAN will forward to LAN 1-4. Therefore, users are able to check VLAN quickly by their functional value as tools for traffic flow.

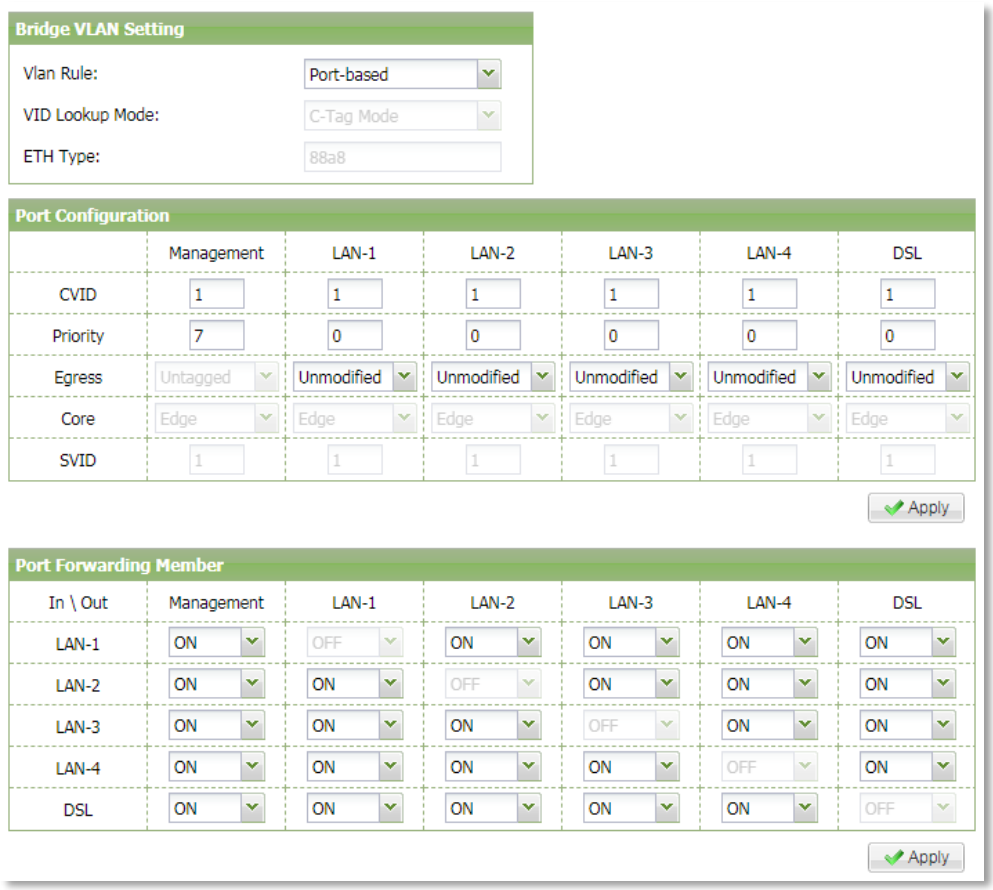


Figure 5-32 Port-based VLAN

- Tag-based VLAN

Tag-based VLAN is based on IEEE 802.1Q. This mode is used to handle traffic in accordance with user-defined forwarding rules that are based on the IEEE 802.1Q tags of the frames. For the external LAN ports, users are able to select whether to discard untagged frames or process them.

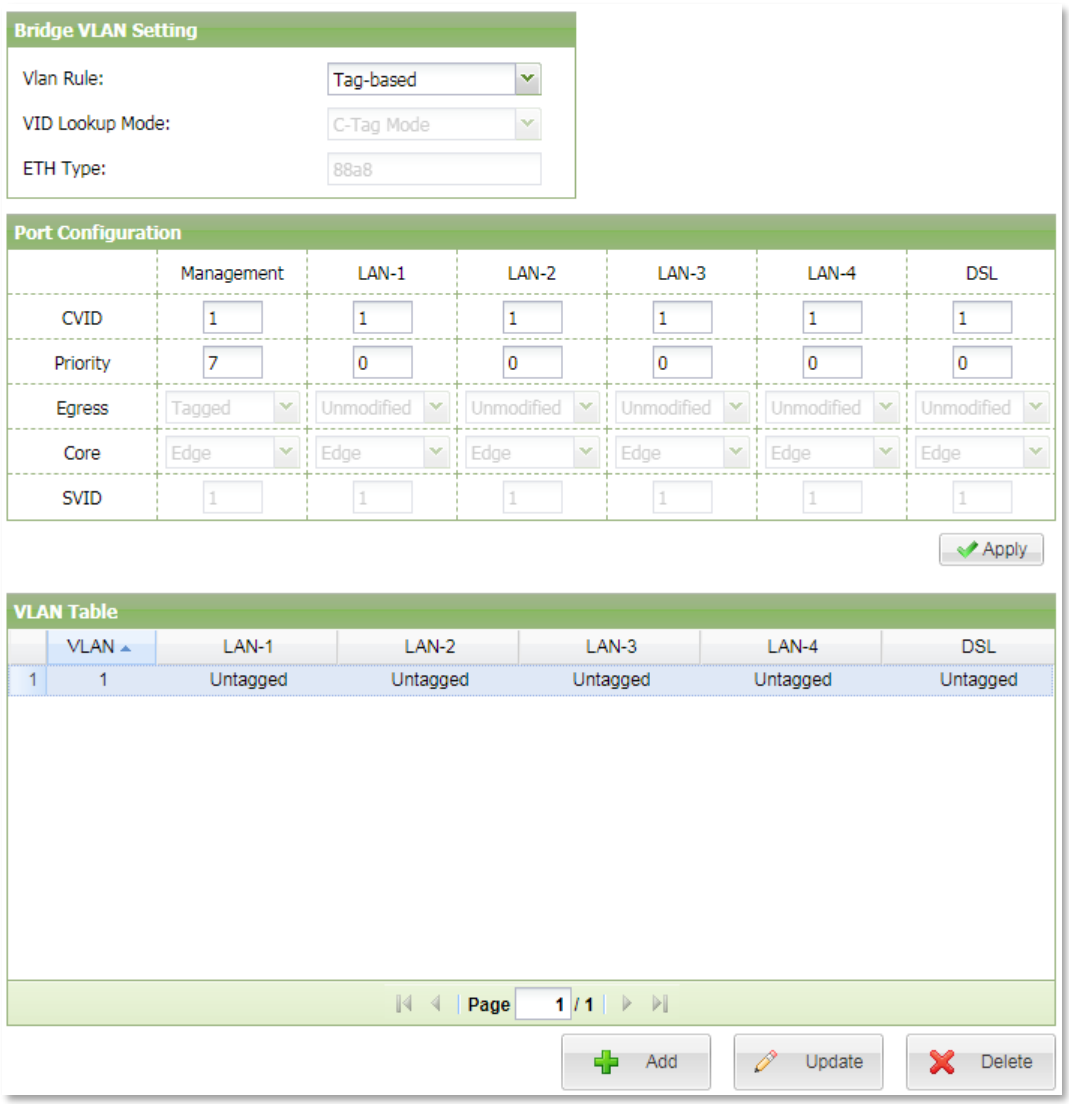


Figure 5-33 Tag-based VLAN

- Q-in-Q

Q-in-Q switching per IEEE802.1ad, is a communication protocol based on IEEE802.1Q. Q-in-Q allows two VLANs to be tagged in the same frame. The main purpose for user is placing a VLAN tag in a VLAN-packet that is identified by an external network without having to change the original packet.

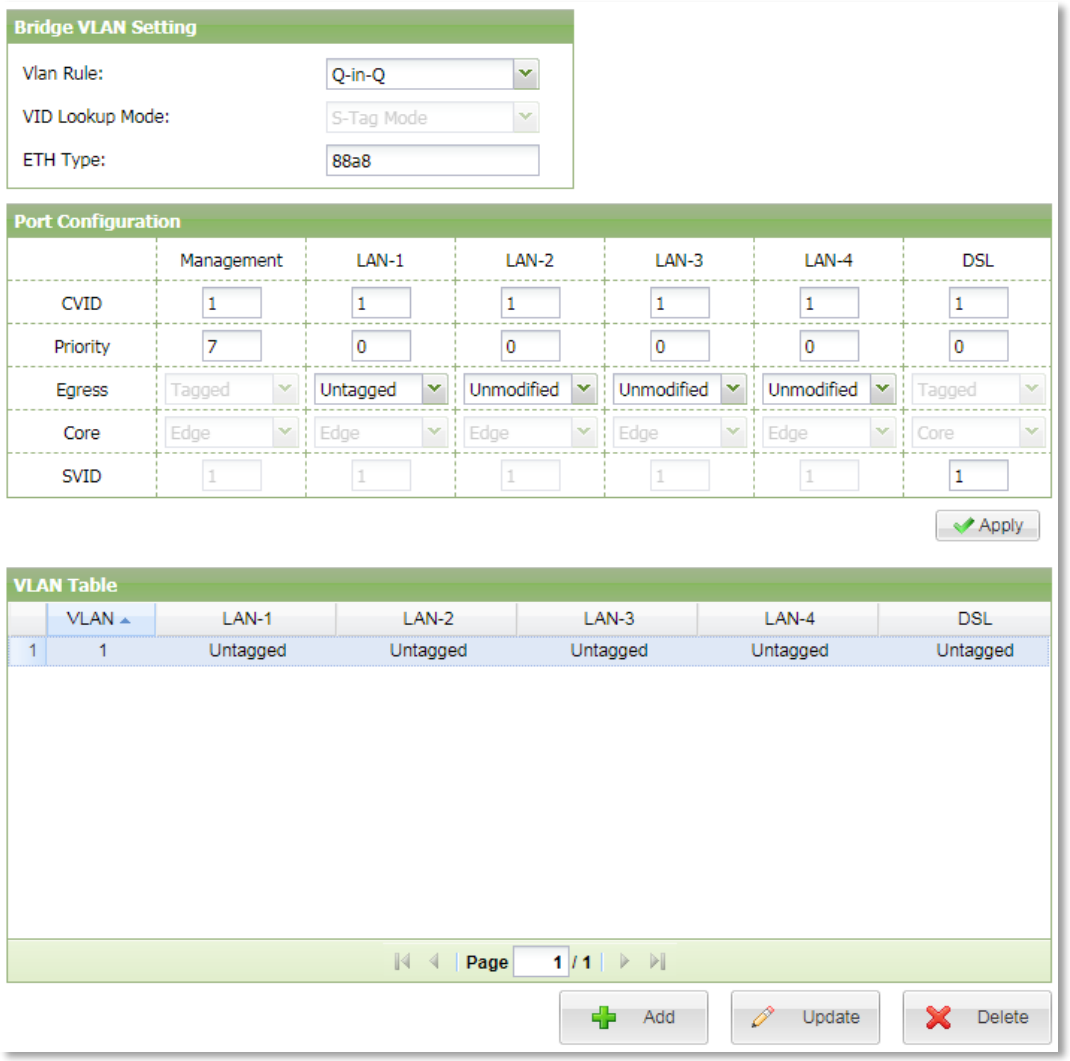


Figure 5-34 Q-in-Q

- **CVID:** Customer VIDs, used for INNER Tag.
- **SVID:** Service VIDs, used for OUTER Tag.
- **TVID:** Target VIDs, used for being Translated Tag.
- **Core:** Working mode as Core (Trunk) port or Edge (Tributary) port.

Note:
When setup it on Q-in-Q mode, the VLAN Tagging is working on double tag mode. The Q-in-Q and VLAN translation CANNOT be used at the same time.

5.5.3 Virtual IP

Firstly, users have to enable "**Tag-based**" in VLAN rule to open the routing mode, and then place any VLANs in VLAN table in order to configure "**Virtual IP**". In Virtual IP table, there are "**Add**", "**Update**" and "**Delete**" functions.

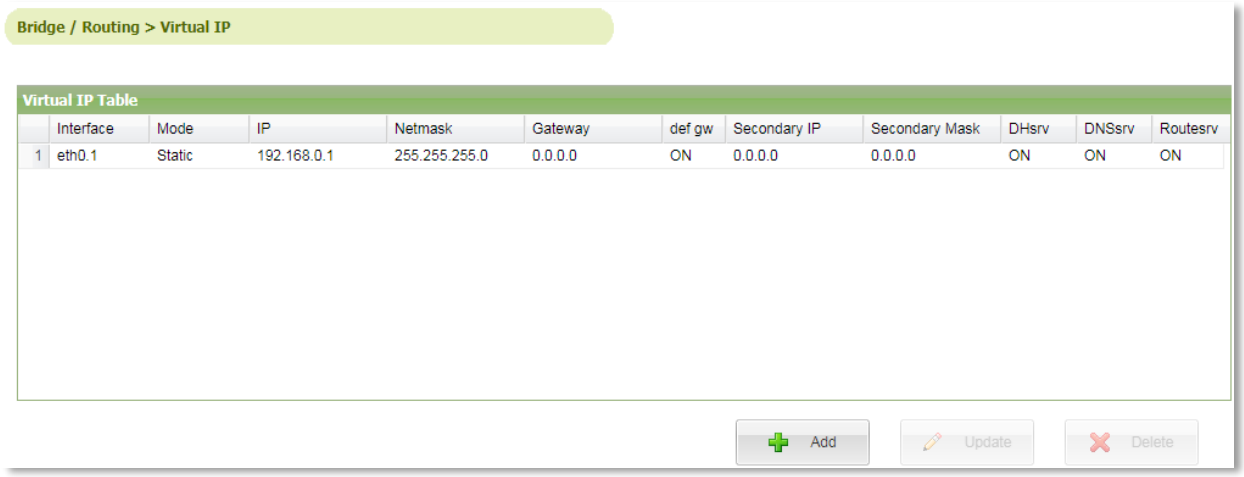


Figure 5-35 Virtual IP

- **Add**: The first parameter is "**VLAN**", configure VLANs which match VLAN table for acting new interface. Operators are able to configure three Modes (Static IP / DHCP client / PPPOE/ PPTP/ L2TP), IP network, default Gateway, secondary IP and so on, based on different application.
- **Update & Delete**: Select IP interfaces in Virtual IP table to update and delete, it is convenient for users to edit rules quickly.

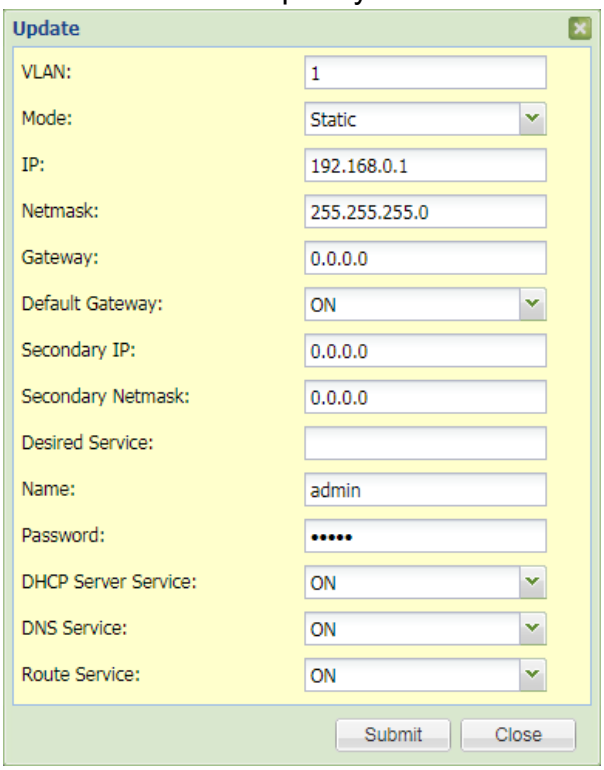


Figure 5-36 Edit Virtual IP

5.5.4 Routing

There are three main tables in this menu, "**Routing Table**", "**Static Route**" and "**Dynamic Route**". Users have to enable "**Tag-based**" or "**Q-in-Q**" in VLAN rule to activate the routing mode.

- **Routing Table**: The default window is "**Routing Table**", to check routing rules conveniently. The rules refer to IP, default gateway from "**Virtual IP**" function. Users can make sure all rules before doing routing application.

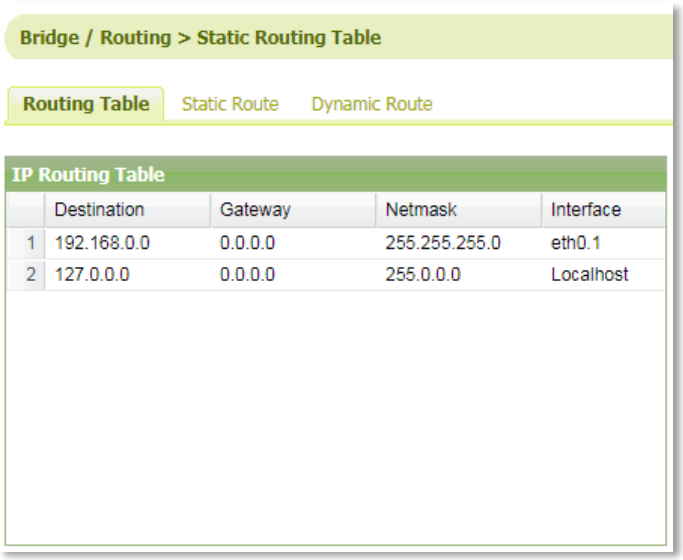


Figure 5-37 Routing Table

- **Static Route**: There are three buttons in this table, "**Add**", "**Update**" and "**Delete**". The main purpose is to manually configure routing rules. It is up to operators' requirements, if operators do not configure it, routing rules will refer to "**Routing Table**". When users start to place a rule in it, remember to configure "Interface" for output interface (eth0.1 or others).

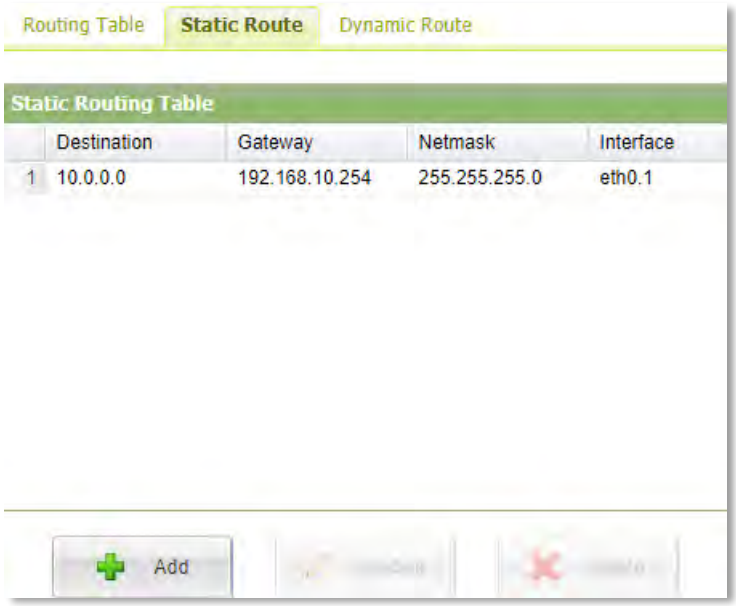


Figure 5-38 Static Route

- **Dynamic Route**: Comet 160xF/ FM and 160xF-R/ FM-R support RIPv1(Classful Routing Protocol) & RIPv2(Classless Routing Protocol), OSPFv2 and BGP4 routing protocol, all network units with RIPv1/v2 in the same network will keep checking each routing rules, but only RIPv2 supports trigger update. While running dynamic

route function, remember that only RIPv2 has VLSM (Variable Length Subnet Masking).

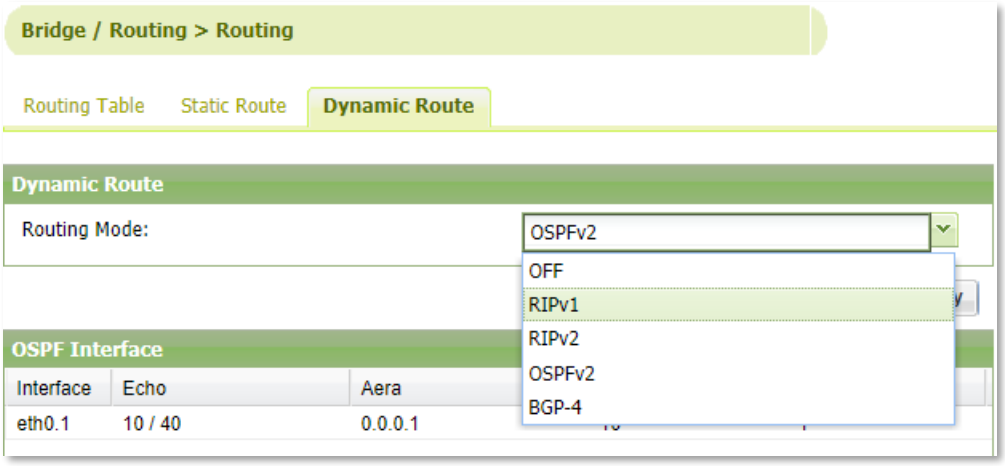


Figure 5-39 Dynamic Route

5.5.5 VRRP

VRRP (Virtual Router Redundancy Protocol) specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

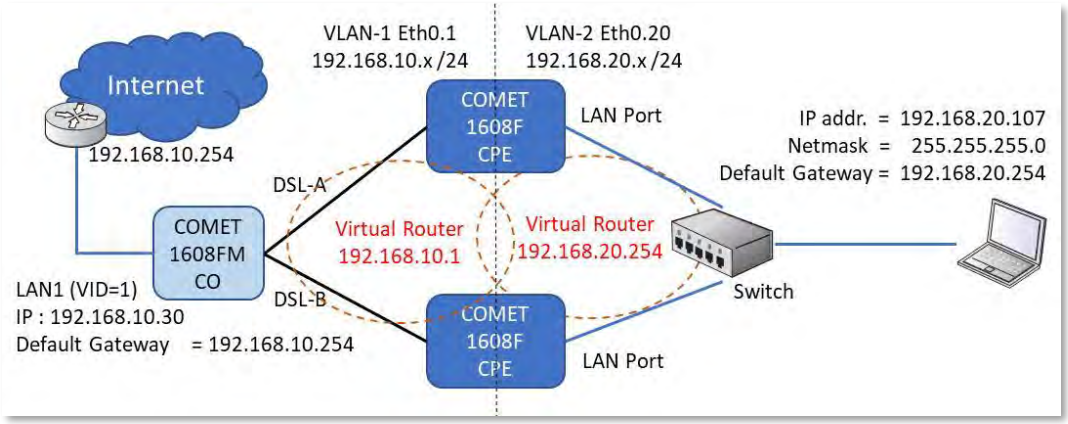
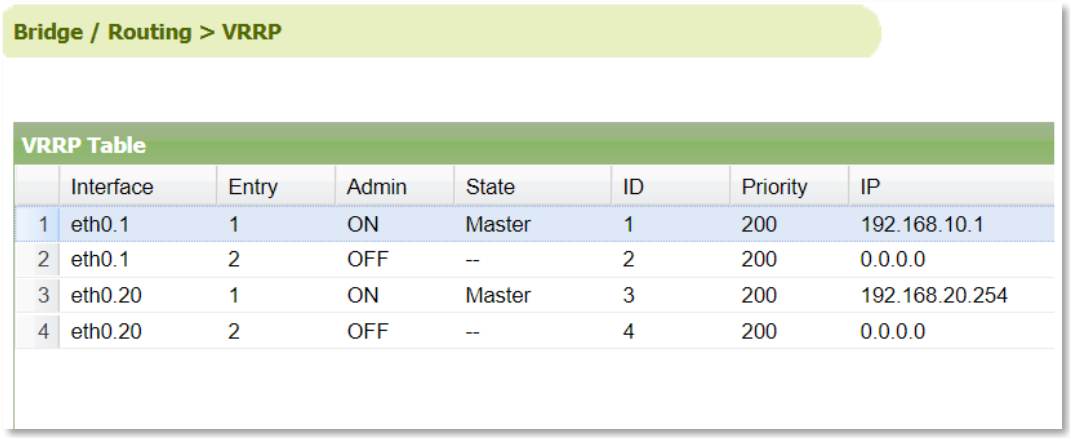


Figure 5-40 Virtual Router Redundancy

The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail over in the forwarding responsibility should the Master become unavailable. This allows any of the virtual routers IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.



Bridge / Routing > VRRP

VRRP Table

	Interface	Entry	Admin	State	ID	Priority	IP
1	eth0.1	1	ON	Master	1	200	192.168.10.1
2	eth0.1	2	OFF	--	2	200	0.0.0.0
3	eth0.20	1	ON	Master	3	200	192.168.20.254
4	eth0.20	2	OFF	--	4	200	0.0.0.0

Figure 5-41 VRRP Table

5.5.5.1 VRRP working on VLAN

Tag based VLAN mode is the entrance point to configure VRRP. It separates the routers interface from WAN to LAN, bundle the DSL(s) together as WAN and joined the different WAN and LAN by different virtual Router ID.

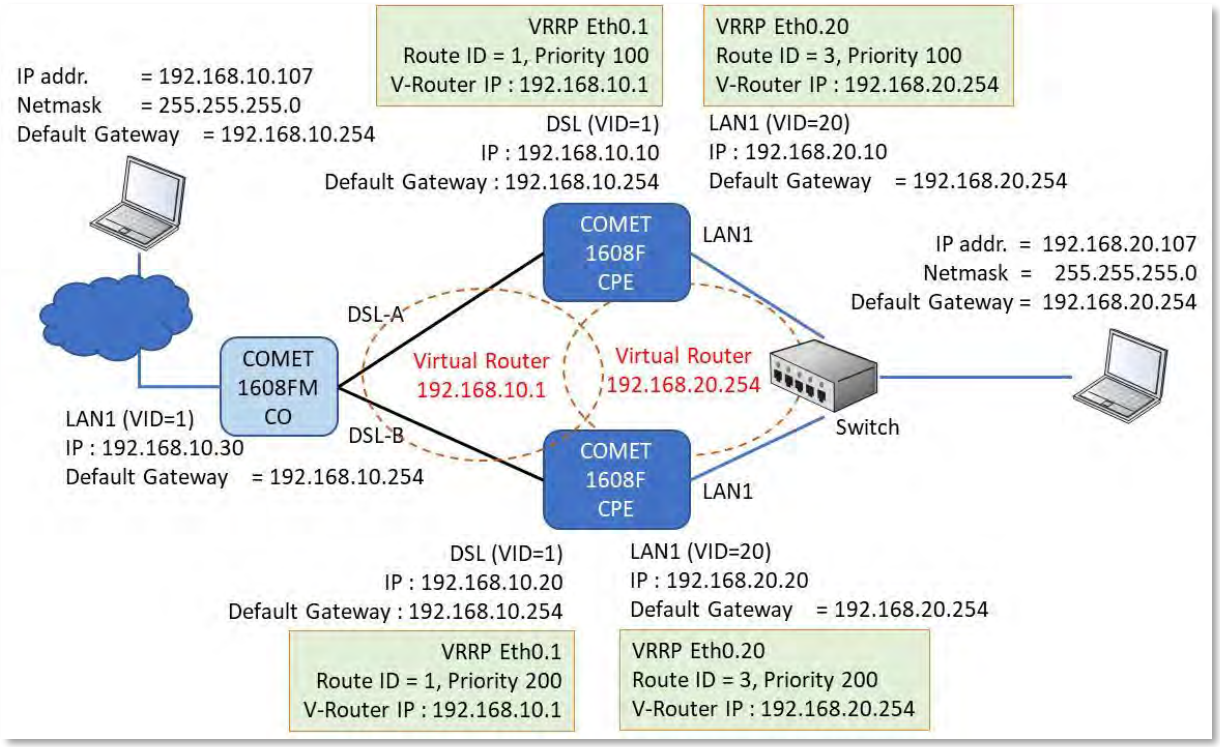


Figure 5-42 VRRP Configuration

5.5.5.2 VRRP Table

After configured the virtual IP on different VLAN segment, the VRRP table will generate two routers interface on each VLAN. The basic VRRP configuration needs only one router interface for each VLAN only. The second router interface is used for additional virtual router to do load balance when needed.

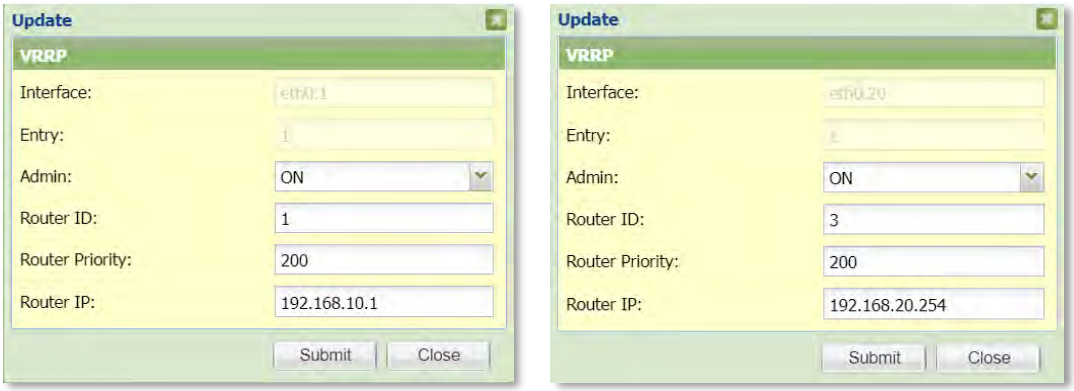


Figure 5-43 Setup VRRP Table

In the previous configuration example, the virtual IP located at VLAN-1 and VLAN-20 is the example for each virtual WAN and LAN routers.

- **Admin**: To turn the virtual router interface ON or OFF.
- **Router ID**: Two physical DSL Routers should apply the same router ID to act as one virtual router.
- **Router Priority**: Two physical DSL Routers apply this priority to switch between "Master" and "Backup" router. The priority number is from lowest 1 to highest priority 254.
- **Router IP**: The virtual router IP address, it is the virtual router for each WAN and LAN routers.

5.5.6 NAT

Users have to enable "**Tag-based**" or "**Q-in-Q**" in VLAN rule to activate the routing mode, and then place VLANs in VLAN table to configure "**NAT**". The default window is "**NAT table**", "**Configuration**" and "**Conntrack Table**" is also in service. For any questions or feedbacks, please contact with TAINET support by E-MAIL: *sales@TAINET.net*

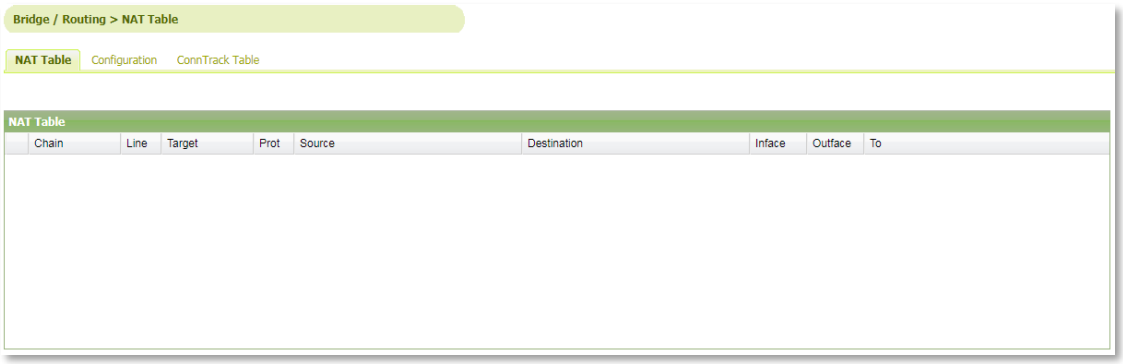


Figure 5-44 NAT Table

5.5.6.1 NAT Table

There are three tabs in NAT table, "**Add**", "**Update**" and "**Delete**". If users would like

to place a NAT rule in it, they are able to click "**Add**" button, or be able to update and delete any rules. For instance, click the "**Add**" button, the menu will display "**Source**", "**Destination**", "**Translation**" and "**To**" four fields.

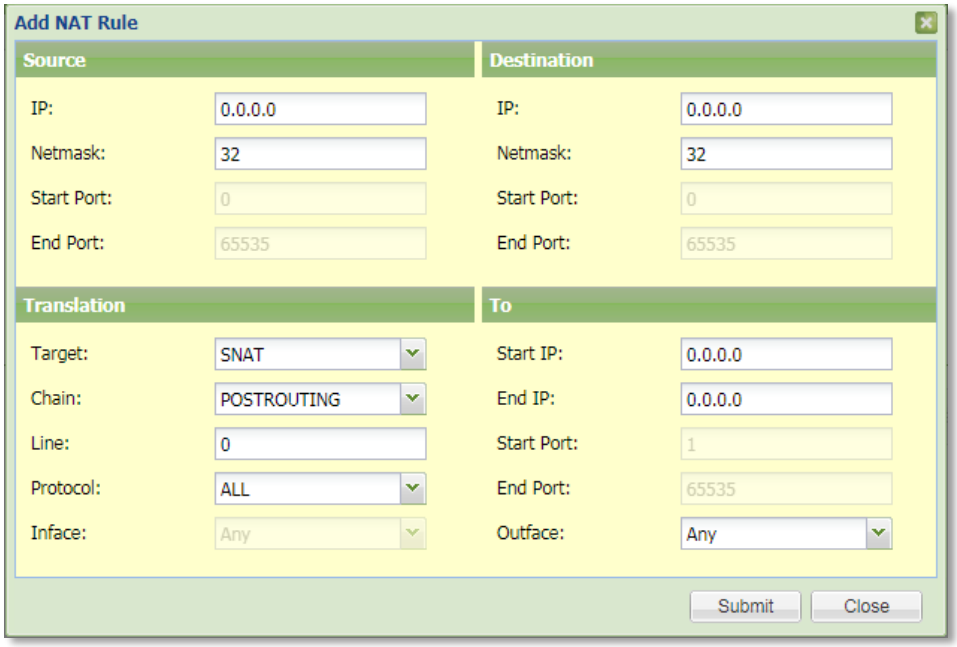


Figure 5-45 NAT Table

To start with, select "**Translation**" to configure **NAT**, **MASQUERADE** or **DNAT**. For default, the "**Target**" is **SNAT**.

- Translation

➢ **Target**: "**SNAT**" (source network address translation), "**MASQUERADE**" (dynamic source NAT) and "**DNAT"** (destination network address translation).

➢ **Chain**: "**POSTROUTING**" appears in SNAT and MASQUERADE, "**OUTPUT**" is only for DNAT to choose output interface.

➢ **Line**: It is the running priority of NAT rule in the NAT table.

➢ **Protocol**: The default is "**ALL**". Others are "**TCP**" and "**UDP"**, only the condition is "**TCP**" or "**UDP**" can activate start to end port number.

➢ **Inface**: It can be only configured by PREROUTING of DNAT mode, choose the interface which refers to "**Virtual IP**".

- Source

➢ **IP**: A specified IP or a range of IPs refers to source side.

➢ **Netmask**: The mask range is from "**0**" to "**32**". For example, Net mask 255.255.255.0 equals to 24.

➢ **Start Port** & **End Port**: Used for a series of TCP and UDP port numbers. It can be only configured as the protocol is not "**ALL**".

- Destination

➢ **IP**: A specified IP or a range of IPs refers to destination side.

➢ **Netmask**: The mask range is from "**0**" to "**32**". For example, Net mask 255.255.0.0

equals to 16.

- **Start Port** & **End Port**: Used for a series of TCP and UDP port numbers. It can be only configured as the protocol is not "**ALL**".

- To

- **Start IP**: To remap the original IP into "**Start IP**" while packets are in transit across a traffic routing device for hiding themselves. The initial IP in the range is "**Start IP**".
- **End IP**: The last IP in the range is "**End IP**".
- **Start Port** & **End Port**: It can be only configured as the protocol is not "**ALL**".
- **Outface**: It can be only configured by SNAT and MASQUERADE mode, choose the interface which refers to "**Virtual IP**".

5.5.6.2 Configuration

- **Max Connection Track:** From "1" to "8192" items
- **Timeout of Established TCP:** From "1" to "432000" seconds
- **Timeout of UDP:** From "1" to "60" seconds
- **Timeout of UDP Stream:** From "1" to "600" seconds

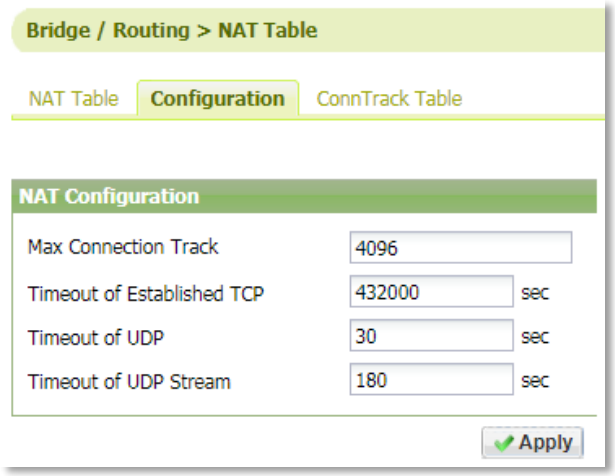


Figure 5-46 NAT Configuration

5.5.6.3 Conntrack Table

"Connection Tracking Table" is very important for network manager to track and observe status of data packages in the transmission network. Conditions contain TCP/UDP, source and destination IP, timeout and connection status.

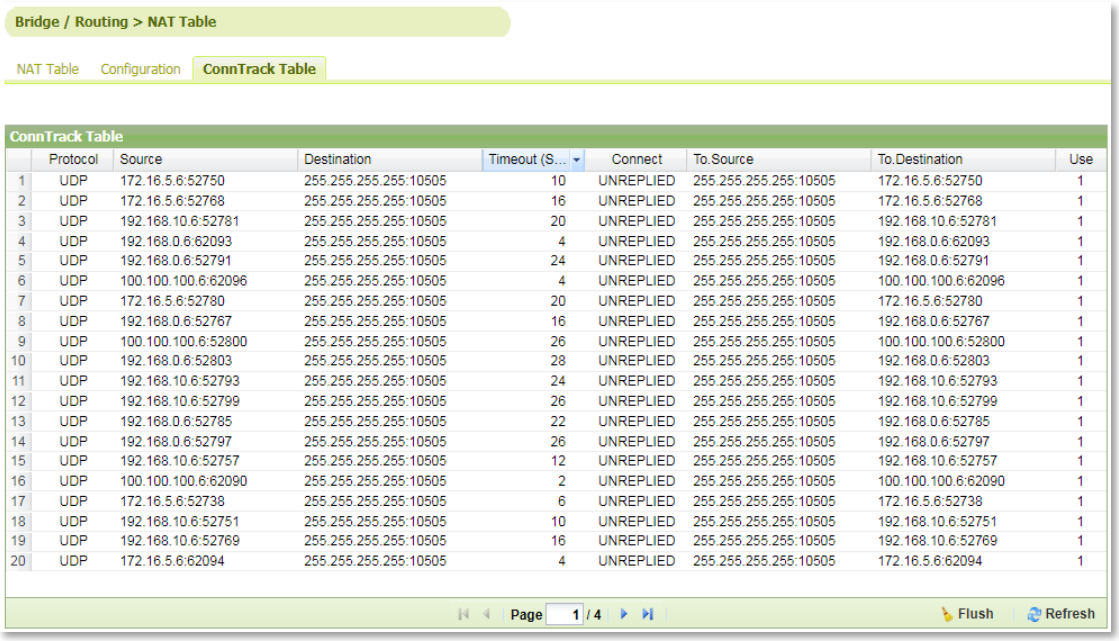


Figure 5-47 NAT Configuration

5.5.7 DNS

DNS is the name service of Internet addresses that translates friendly domain names to numeric IP addresses. Comet 16xxF/160xFM and 160xF-R/ FM-R support DNS Server & DNS cache. Firstly, users have to enable "**Tag-based**" in VLAN rule to activate the DNS function. If the modem acts as DNS Server, enable the "**Authoritative Server Mode**". Or if users would like to follow outside DNS servers, enable the "**Domain Name Service Mode**".

- Domain Name Service Configuration

➢ **Domain Name Service Mode**: "**Cache**" (DNS cache), "**OFF**" (Disable DNS)
➢ Domain Name Service Name: The default service name is "dev_MAC address".
➢ **Timeout (sec)**: It is time interval of transmitting DNS packages.
➢ **Upstream Server-1**: Default IP is "**8.8.8.8**" refers to outside DNS server-1.
➢ **Upstream Server-2**: Default IP is "**8.8.4.4**" refers to outside DNS server-2
➢ **Authoritative Server Mode**: "**ON**" (Specified DNS Server), "**OFF**" (Random bypass)

- Authoritative Server Zone

Users will be able to "**Add**", "**Update**" and "**Delete**" specified DNS server rules. Here prepares an example in Page 1 for references.

Zone 1 | myexample-1.net
Zone 1.1 | www.myexample-1.net <=> 192.168.0.1 +86400
Zone 1.2 | mail.myexample-1.net <=> 192.168.0.1 +86400

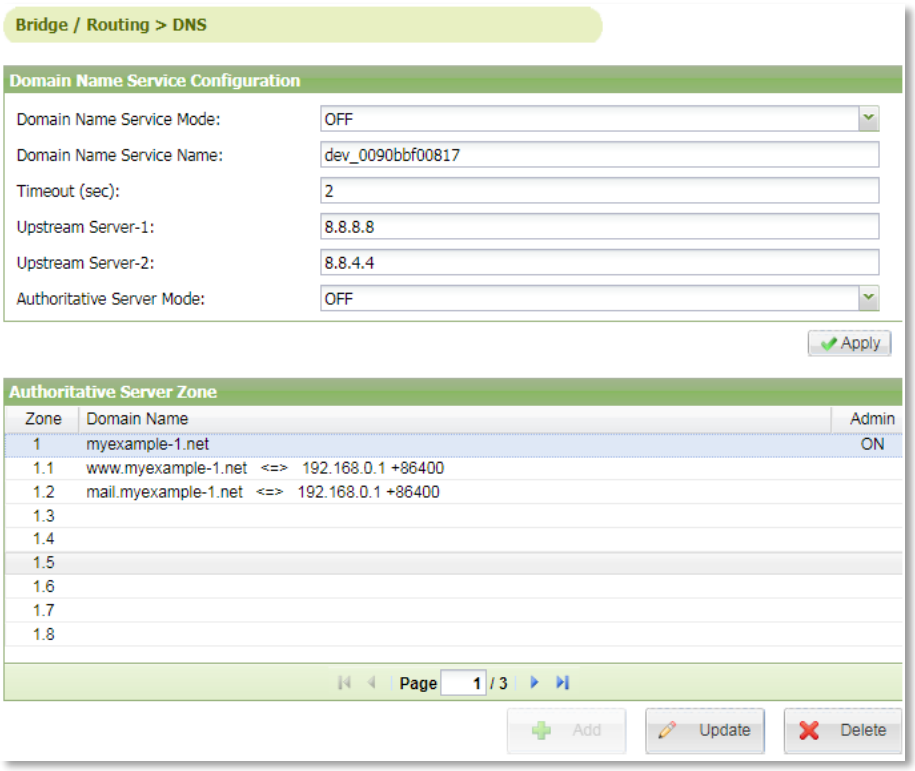


Figure 5-48 DNS Server/Cache

5.5.8 G.8032

Comet 160xF/ FM and 160xF-R/ FM-R provides ERPS (Ethernet Ring Protection Switch) according to ITU-T G.8032 standard. With this feature, it can complete two topologies, the way for connecting each device not only basic serial linear network but also ring topology. Downside of serial linear network is stability of any nodes between traffic would affects the whole network. Ring network can resolve the issue because of redundant system. Besides, the ring protection is established in ETH switch or DSL trunk.

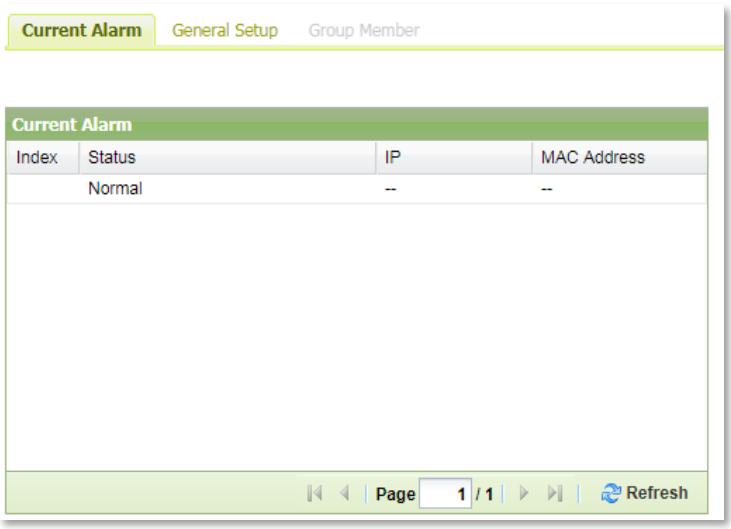


Figure 5-49 Current Alarm

- Current Alarm

  When current Ethernet packets loop alarms occurred, logs will be displayed and updated immediately in this form. "**Normal**" means the ring topology has been completed with no errors.

- General Setup

➢ **Admin**: Select "**Enable**" to run G.8032.

➢ **UDP Port**: Default UDP port number is "**30000**".

➢ **Ring Number**: Default ring number is "**0**", set all devices with the same number in ring network.

➢ **Interface**: Select Ethernet interface for data output.

➢ **Character**: Only one unit is "**Owner**", the others are "**Member**". When a device is set to "**Owner**", it becomes central unit with more abilities that can decide others would join in the ring network or not.

➢ **Owner MAC Address**: Users can assign members to the specific owner, or accept the automatic allocation by default MAC address.

➢ **Link-0**: In ring network, each unit needs at least two physical lines to connect other two units. Choose LAN-1 to LAN-4 for doing Ethernet ring network, or DSL L1~L4 (Comet 1608FM p-to-mp 2w mode) or DSL Port A/B (Comet 160xFM) for doing DSL ring network.

➢ **Link-1**: Refer to the description of Link-0.

➢ **Ring Protection Link**: Select one data trunk to be ring protection, to avoid loop errors. The chosen one will be shut down in the beginning, while other trunks in this network is being destroyed, the mechanism will automatically enable the chosen one to recover the whole transmission.

Note: Remember to configure the parameter at both ends of Comet 160xF/ FM and 160xF-R/ FM-R.

➢ **Broadcast**: Two types of Broadcasts, "**Local**" and "**Global**" would follow the configuration of device IP and Subnet Mask.

➢ **Packet Repeat**: Default packet repeat is "**0**". The number of times packets have repeated.

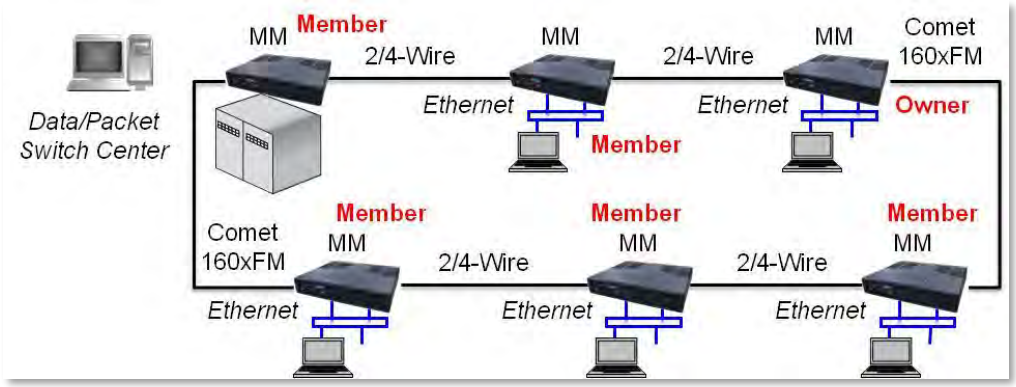


Figure 5-50 Owner and Member for Ring toplogy

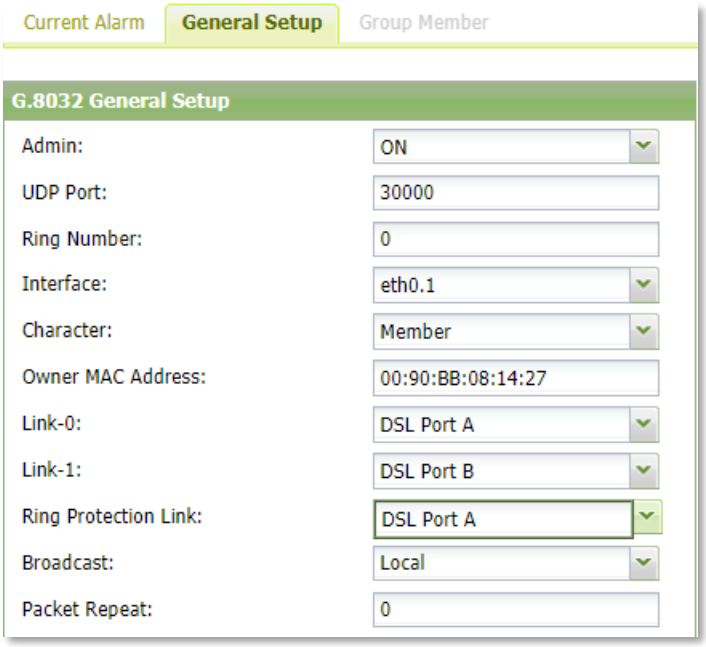


Figure 5-51 General Setup

- Group Member

  When the device is "Owner", users are able to check all online "Member" in this form. Click "Add all candidate" to add members to G.8032 Group Member.

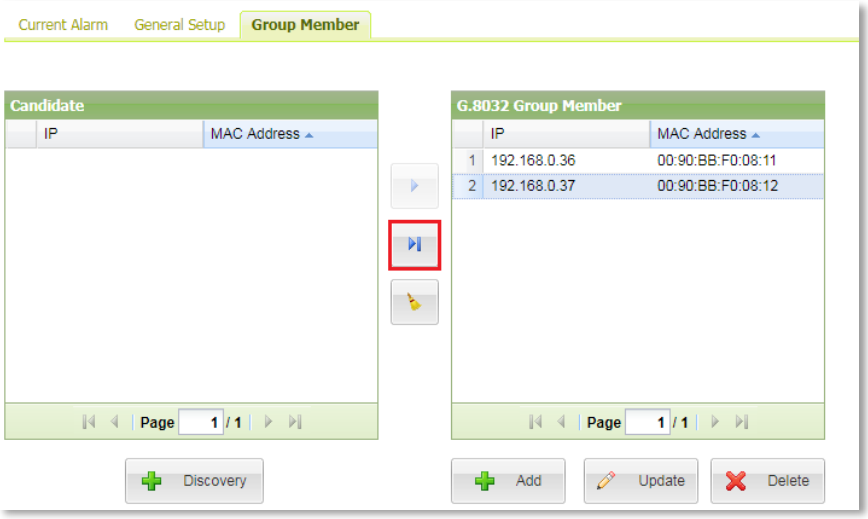


Figure 5-52 Group Member

5.5.9 RSTP

Since software version V1.306, Comet 160xF/ FM and 160xF-R/ FM-R provides RSTP (Rapid Spanning Ring Protection) according to IEEE 802.1w standard. With this feature, it can connect each device in linear, ring or mesh topology and prevent the traffics broadcast storm in loop.

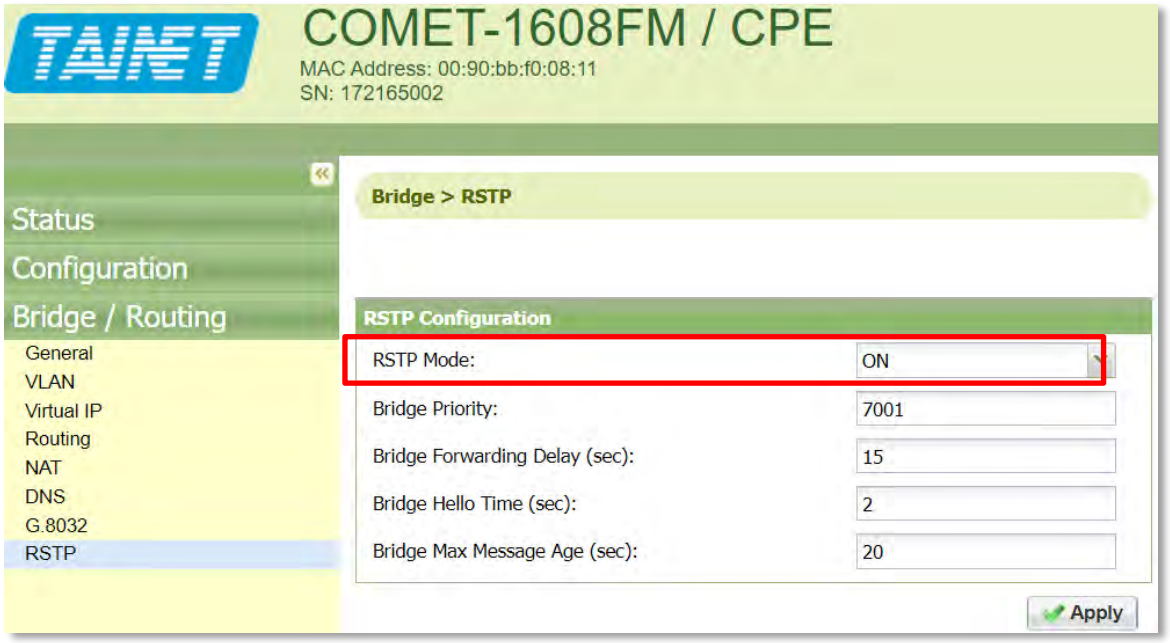


Figure 5-53 Rapid Spanning Tree Protocol (RSTP)

RSTP use BPDU (Bridge Protocol Data Unit) to exchange information about Bridge IDs and root path costs between Ethernet switches. BPDUs are exchanged regularly (every 2 seconds by default), enable the switches to keep track of network changes and to start or to stop forwarding at ports as required.

- **Bridge Priority:** The Bridge ID (BID) has eight bytes in length, is a field inside a BPDU packet. The first two bytes are the bridge priority, an unsigned integer of 0-65,535. The last six bytes are a MAC address supplied by the bridge.
- **Bridge Forwarding Delay:** When a device is first attached to a switch port, it will not start to forward data immediately. It will go through a number of states instead while it processes BPDUs and determines the topology of the network. The time spent in the listening and learning states determined by a value known as the forward delay (default 15 seconds and set by the root bridge).
- **Bridge Hello Time:** RSTP is typically able to respond to changes within 3 × Hello times or within a few milliseconds of a physical link failure. The Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 3 times with 2 seconds for each.
- **Bridge MAX Message Age:** As soon as loop happens in RSTP Count to Infinity, the message age is like a mechanism to avoid a loop. The maximum message age timer specifies the maximum expected arrival time of hello BPDUs. If the maximum message age timer expires, the bridge detects that the link to the root bridge has failed and initiates a topology re-convergence. The maximum message age timer should be longer than the configured hello timer.

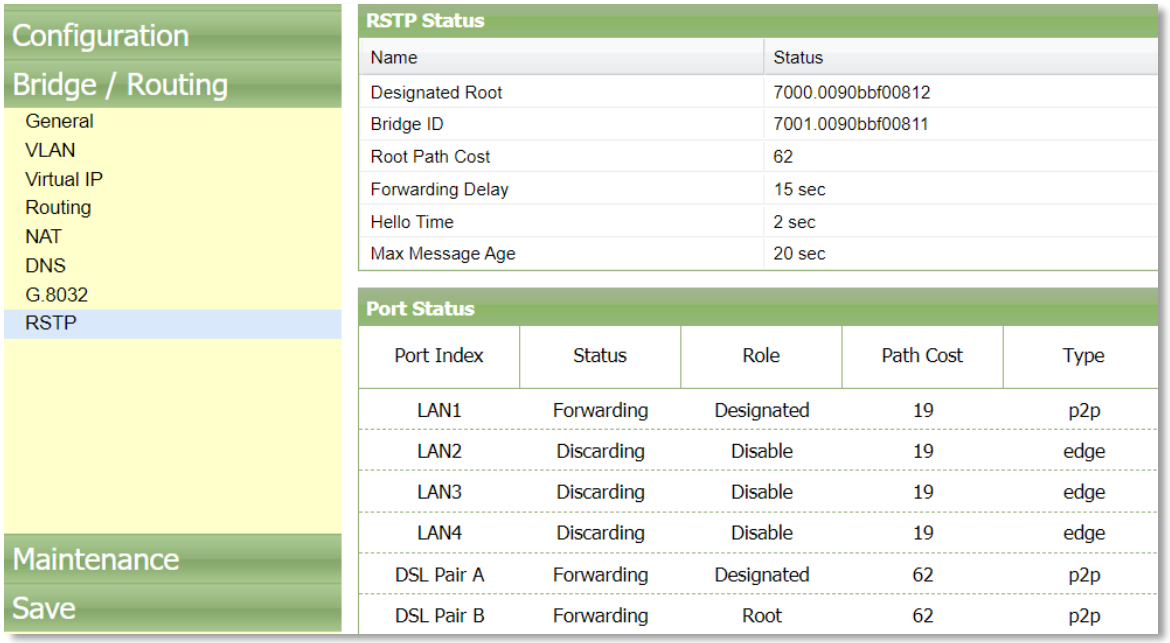


Figure 5-54 RSTP Status and Port Status

- **Designated Root:** The status item shows information of Root Bridge. Include its Bridge Priority cost value and MAC address followed.
- **Bridge ID:** This status row shows information of this bridge itself. Include its own Bridge Priority cost value and MAC address followed.
- **Root Path Cost:** The Cost Value is inversely proportional to the associated bandwidth of the path. A path with a lowest cost value in this switch network is assigned as owned by Root Bridge. A network in the same segment has one and only one Root Bridge.

Table 5-3 Port Status of RSTP

STP	RSTP	Port Active	MAC Learning
Disable	Discarding	No	No
Blocking		No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

- Port Status
- **Forwarding:** The MAC address is learning and forwarding.
- **Learning:** The Learning state appears in a short period of time during Alternate Port and Backup Port is going to replace Root port.
- **Discarding:** The Disable, Blocking and Listening port state in STP is the same as discarding port state in RSTP now.
- Port Role
- **Root Port**: The port with shortest path to the **Root Bridge** is called root port.

- **Designated Port**: Except the root port, the port with second shortest path to the root bridge is Designated Port.
- **Alternate Port**: is an alternate path that receives better BPDU from another switch. It is the backup of Root Port.
- **Backup Port:** is a blocking port that receives better BPDU from the same switch. It is the backup of Designated Port. If Alternate Port and Backup Port exist in the same network segment, the Backup Port has higher priority to replace Designated Port when Designated Port failed.
- **Disable Port:** Without any connection or the connection is broken in this moment.

● Port Type

- **Edge Port**: The edge port can change to Forwarding state with no delay. It does not go through the Listening and Learning state.
- **P2P Port:** A port that operates in full duplex is assumed to be point-to-point.
- **Share Port:** While a half-duplex port is considered as a shared port by default.

5.6 Maintenance

5.6.1 Local/ Remote Alarm Log

The alarm history is displayed in this section. Network manager can check different severity levels of logs in different system time.

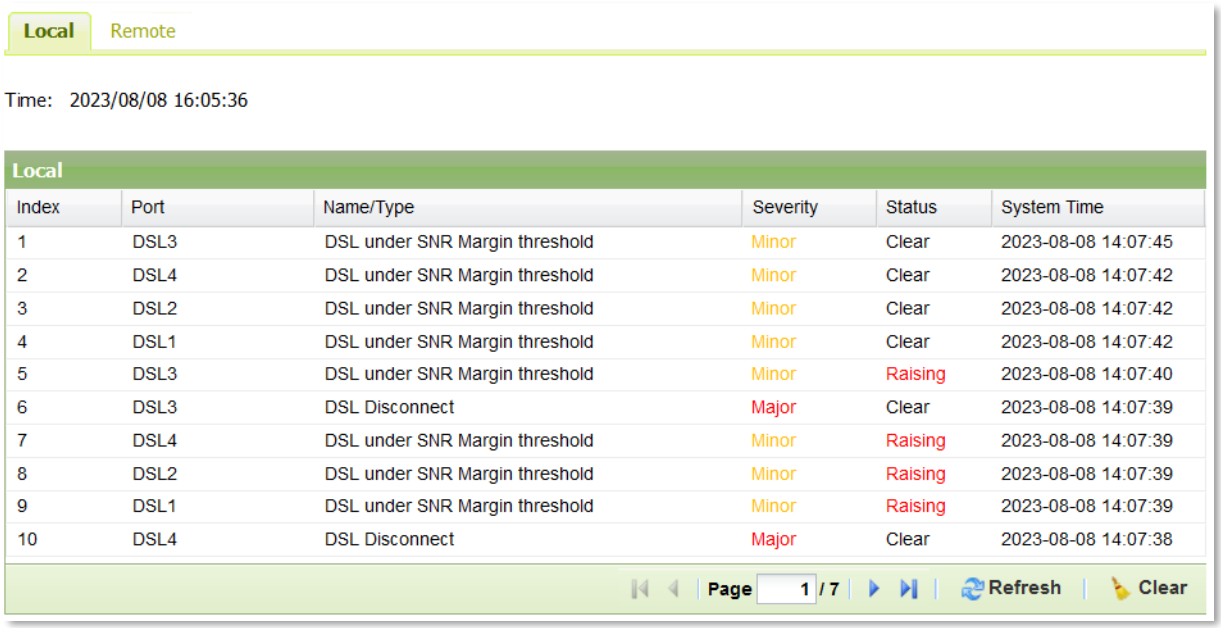


Figure 5-55 Alarm Log

5.6.2 Local/ Remote Access Log

All IP accessed and WEB action logs are displayed in this section. Network manager

can check all operation records in the past time.

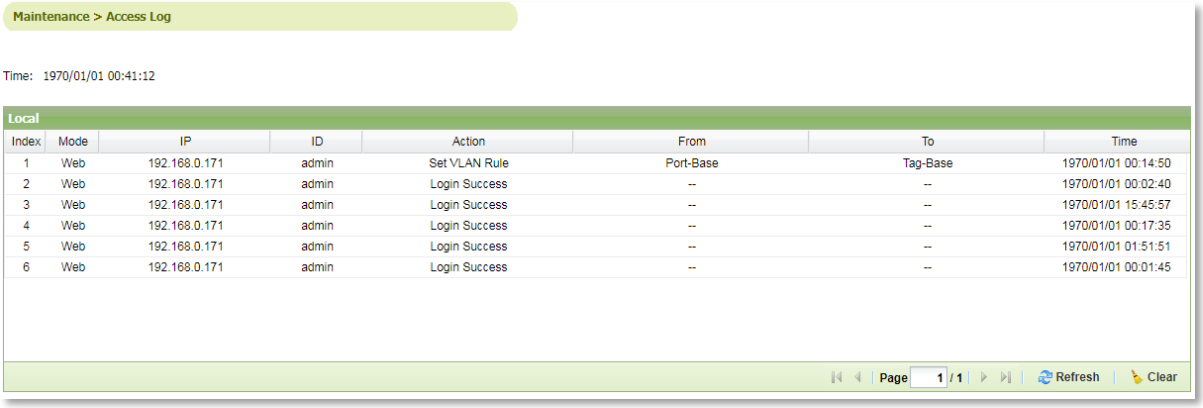


Figure 5-56 Access Log

5.6.3 Account Protection

System displays the unauthorized IPs. When the wrong authentication is entered in the login screen over 5 times, Comet 160xF/ FM and 160xF-R/ FM-R will refuse the IP address. Manually clear the table records will recover the block IPs.

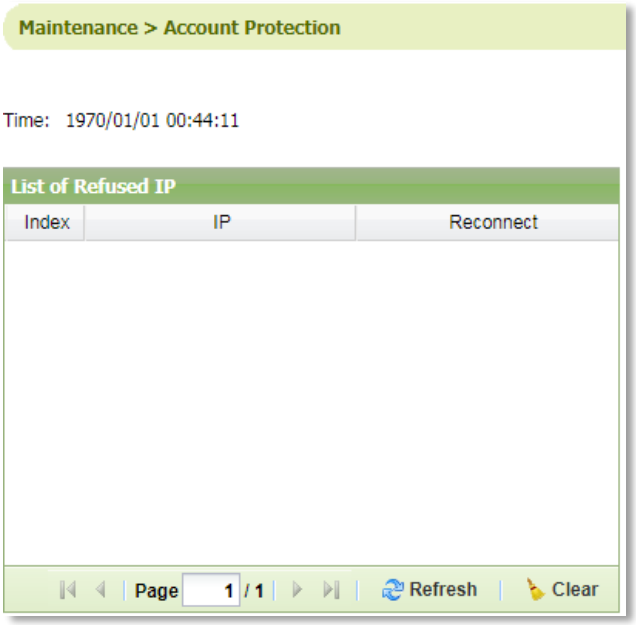


Figure 5-57 Account Protection

5.6.4 Performance History

The performance history shows the errors occurred on each subscriber loop within 15 minutes or 1 day duration. The system supports local/ Remote G.SHDSL performance history. Users can manually update all records.

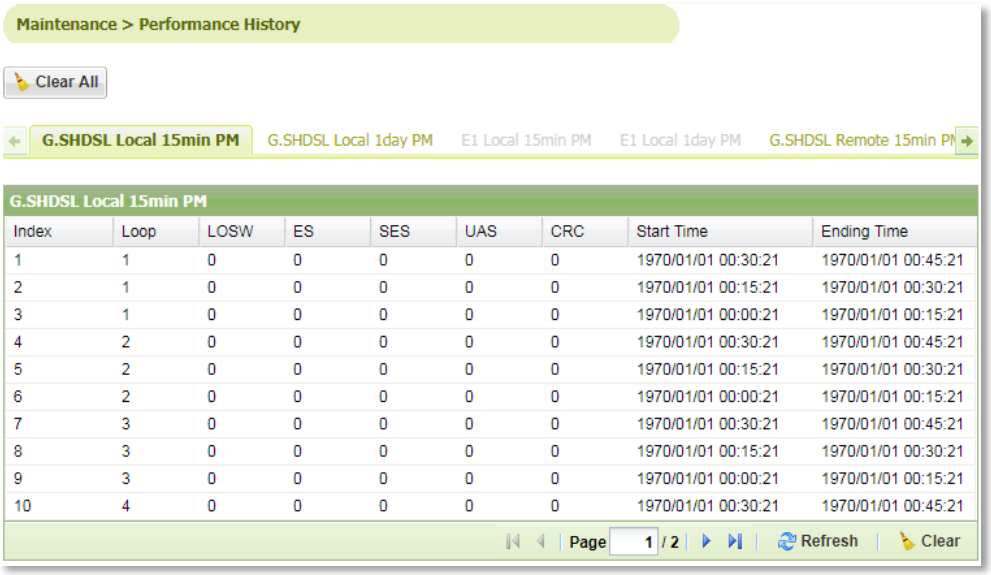


Figure 5-58 Performance History

5.6.5 Ethernet Statistics

The following information shows, Counter Name, RX Packet Counts, RX Packet Bytes, TX Packet Counts, TX Packet Bytes, Error Counts and Collision Counts.

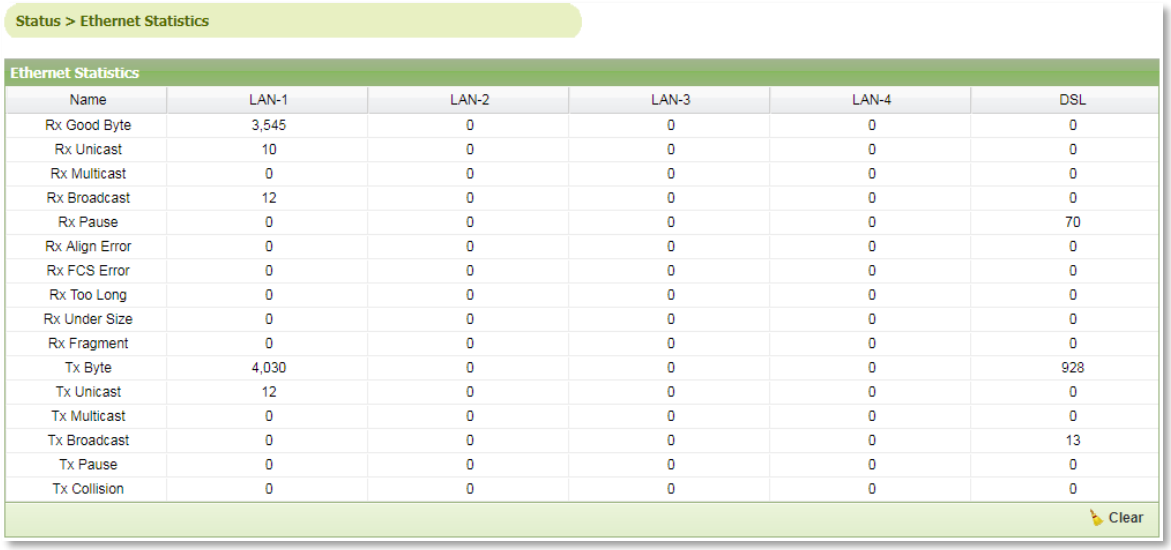


Figure 5-59 Ethernet Statistics

5.6.6 Software Default

This function is used to restore all settings to factory defaults besides device IP, VLAN and management authority.

After clicked the "Apply" button, the pop-up window will show the confirmation message.

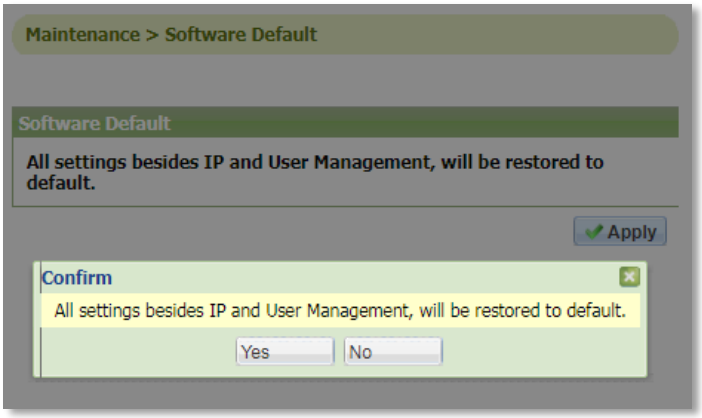


Figure 5-60 Software Default

5.6.7 Factory Default

This function is used to restore all settings to factory defaults including device IP, VLAN and management authority which software default does not change.

After click the "Apply" button, the pop-up window will show a message to reconfirm.

Figure 5-61 Factory Default

5.6.8 Software Upgrade

The local device can be upgraded by HTTP, and users have to select the correct firmware code for uploading.

Step 1: Click "Browse" to open folder and get the AP image file for upgrade.

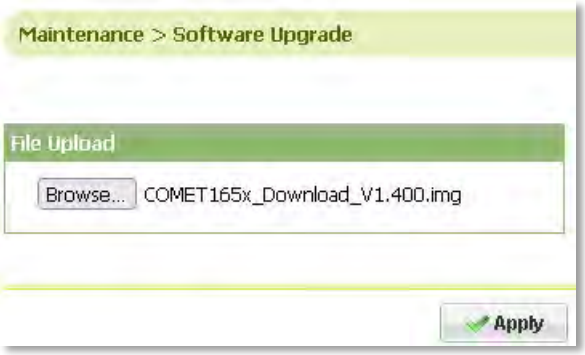


Figure 5-62 HTTP File Upload

Step 2: Select "**OK**" to save all current configurations.

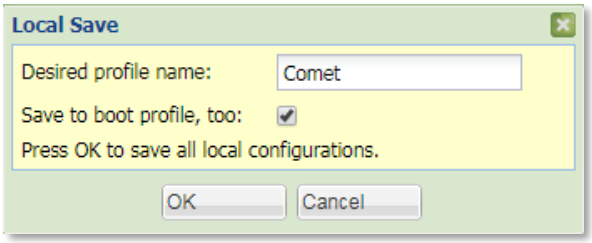


Figure 5-63 Local Save

Step 3: The system will start to detect the new firmware code.

Figure 5-64 HTTP Uploading File

Step 4: Select "Yes" to upgrade the version, there are 20 seconds for operators to check version information and upgrade confirmation.

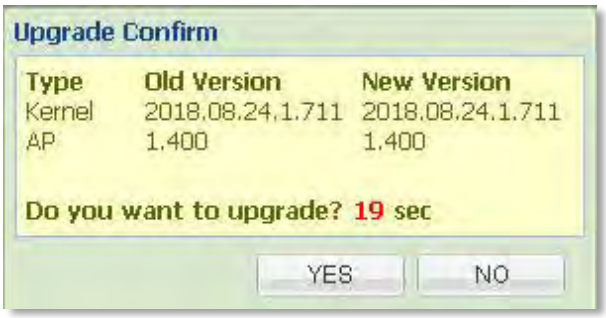


Figure 5-65 HTTP Upgrade Version Confirmation

Step 5: During upgrade processing, all LEDs on devices' front panel will blink at the same time. Do not turn off the power during its proceeding and the total procedure will take about 3 minutes to go back to standby mode.

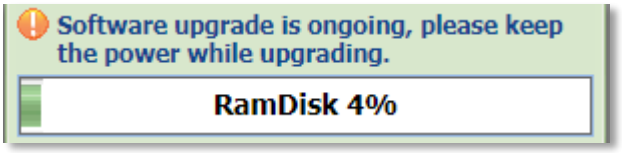


Figure 5-66 Upgrade Proceeding

5.6.9 SSL Setting

SSL supports a security way to access Comet 160xF/ FM and 160xF-R/ FM-R. By using HTTPs to access WEB is able to protect devices from hacking attempt. To improve the security level of modem, TAINET provides three types of SSL certification.

SSLCaCertificateFile(.crt)

SSLCertificateFile(.crt)

SSLCertificateKeyFile(.key.pem)

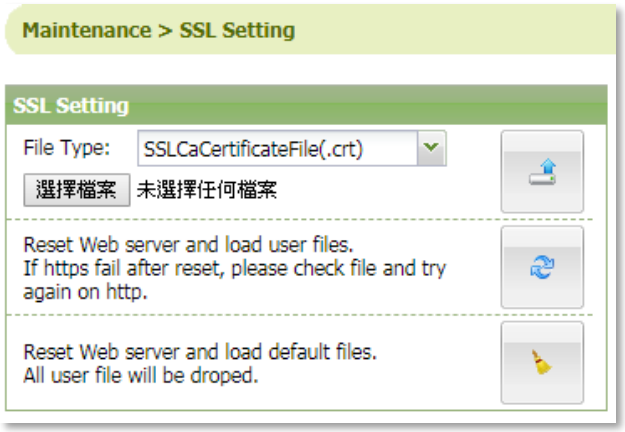


Figure 5-67 SSL Setting

5.6.10 Ping

The feature is used to verify the path of packet transmission is reachable or is alive. User may select "**Interface**" for path and input an IP address in "**Ping IP**" to test.

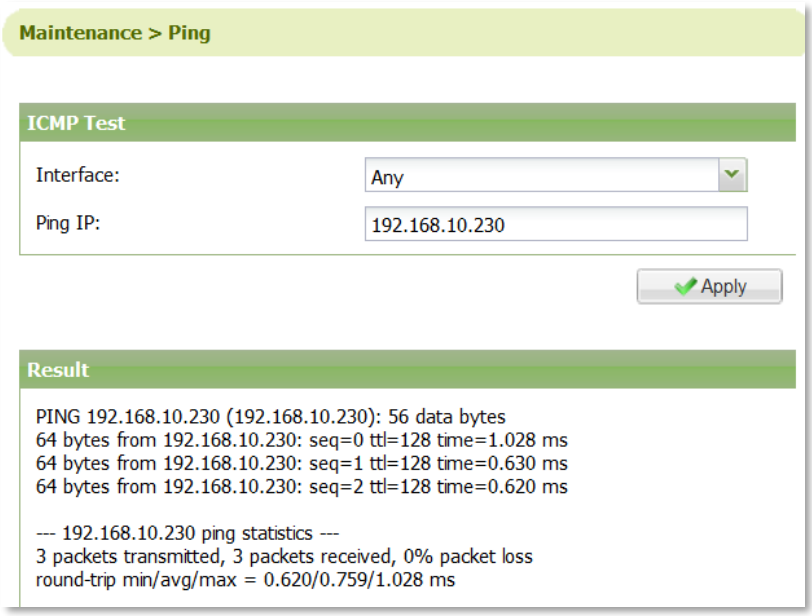


Figure 5-68 Ping

5.7 Save

5.7.1 Local/ Remote Save

Save all Local/Remote configurations to user profile. This way will help Comet 16xxF/ 160xFM and 160xF-R/ FM-R to save current configuration and restore this profile for next power on.

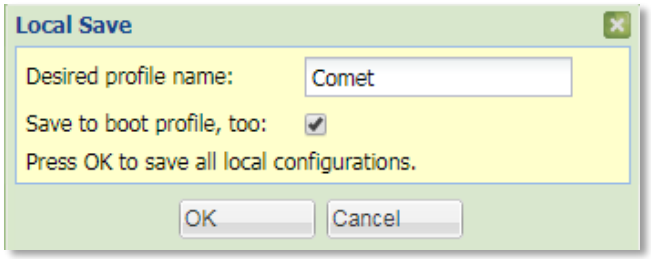


Figure 5-69 Local / Remote Save

5.8 About

5.8.1 Software Version

The system will show the correct model type and software version of Comet series on local and remote (Comet 16xxF only) modems.

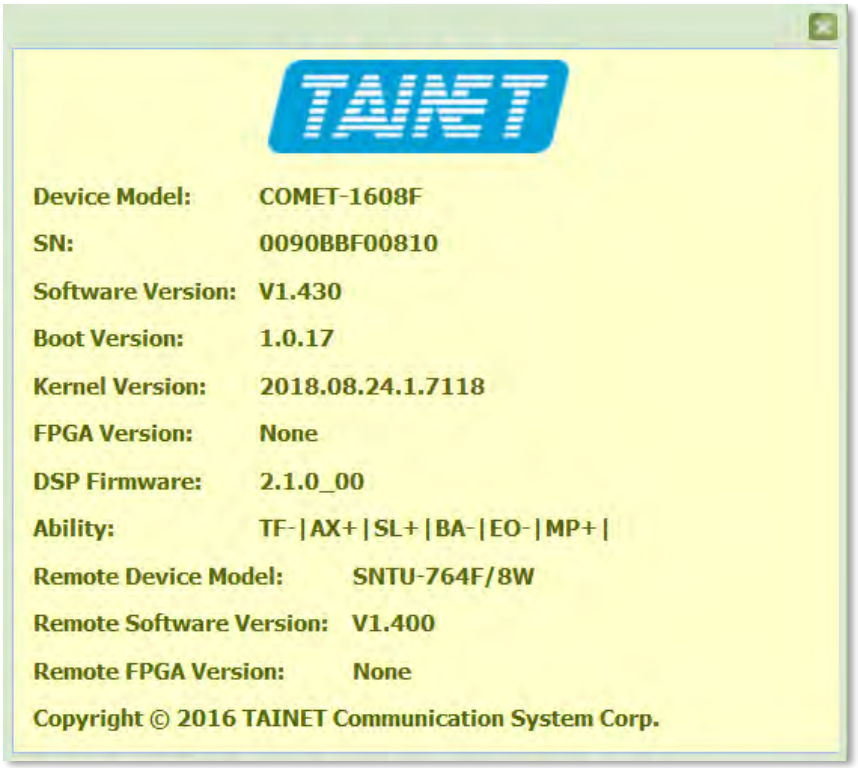


Figure 5-70 Local Software Version

5.9 Action

Figure 5-71 Action

- **Logout**: Return to the login page.
- **Local System Reboot**: Restart the local modem.
- **Remote System Reboot**: Restart the remote modem (Comet 160xF only).
- **Summary**: Operator can upload a summary file includes of all configurations, modem status, alarm log, and Ethernet statistic to local storage. It can be analyzed by network manager for further assistance.

5.10 Application Examples

5.10.1 Bridge ATM Application

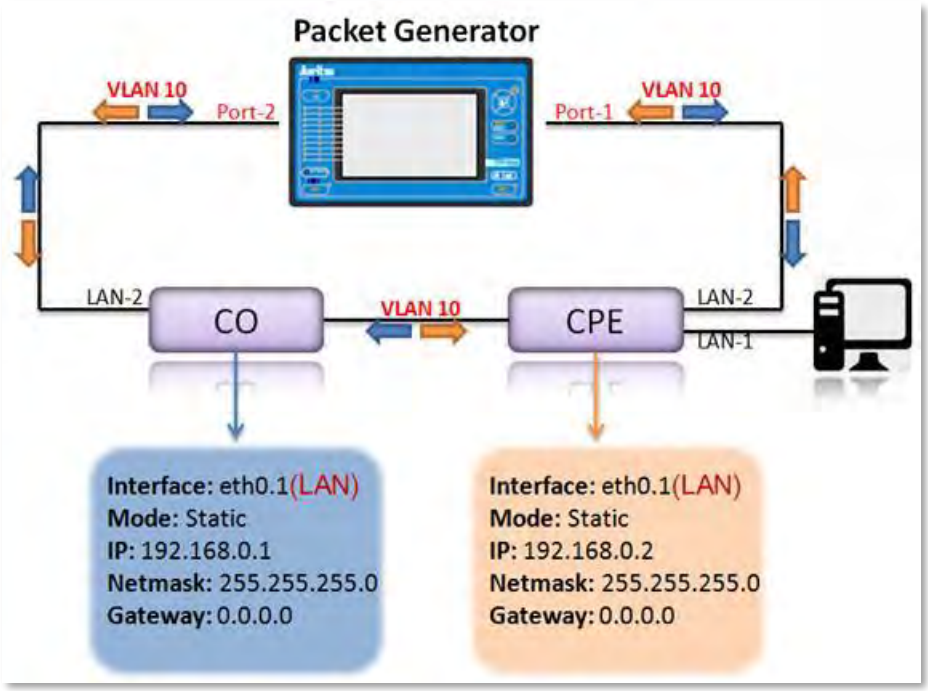


Figure 5-72 Bridge ATM Application

- < CO configuration >

1. Configuration > Local Setting > G.SHDSL

Mode= **ATM** / Side Mode= **CO** / Wire Mode= **8w**

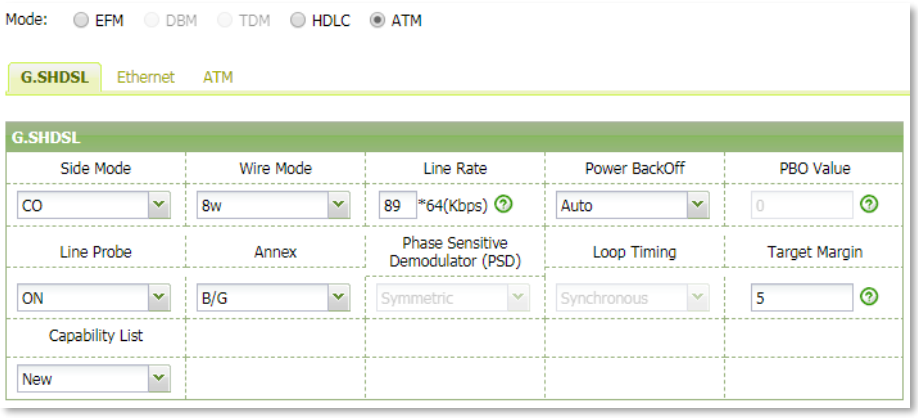


Figure 5-73 CO-G.SHDSL

2. Configuration > Local Setting > ATM

Index 2: VID=**10** / VPI=**7** / VCI=**2000**

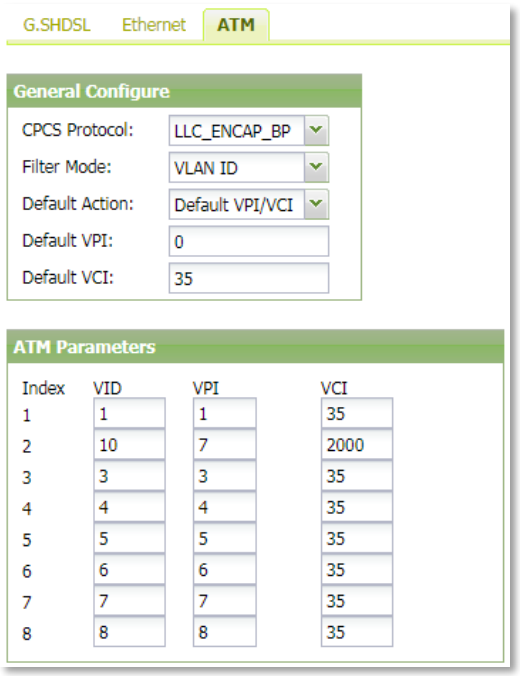


Figure 5-74 CO-ATM

3. Bridge / Routing > VLAN

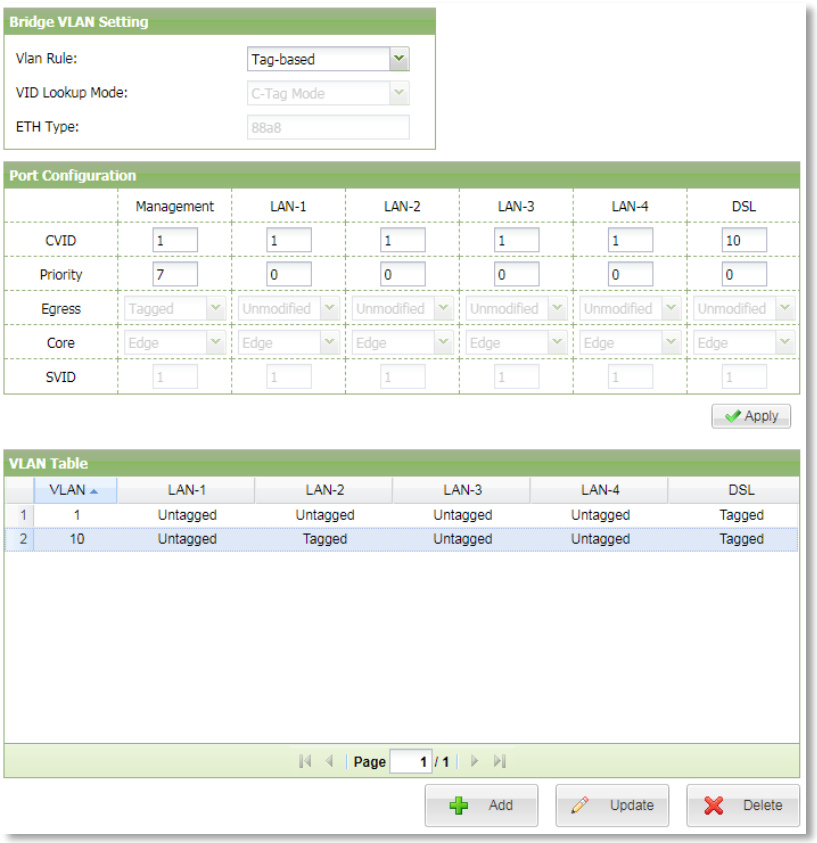


Figure 5-75 CO-VLAN

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

Mode= **ATM** / Side Mode= **CPE** / Wire Mode= **8w**

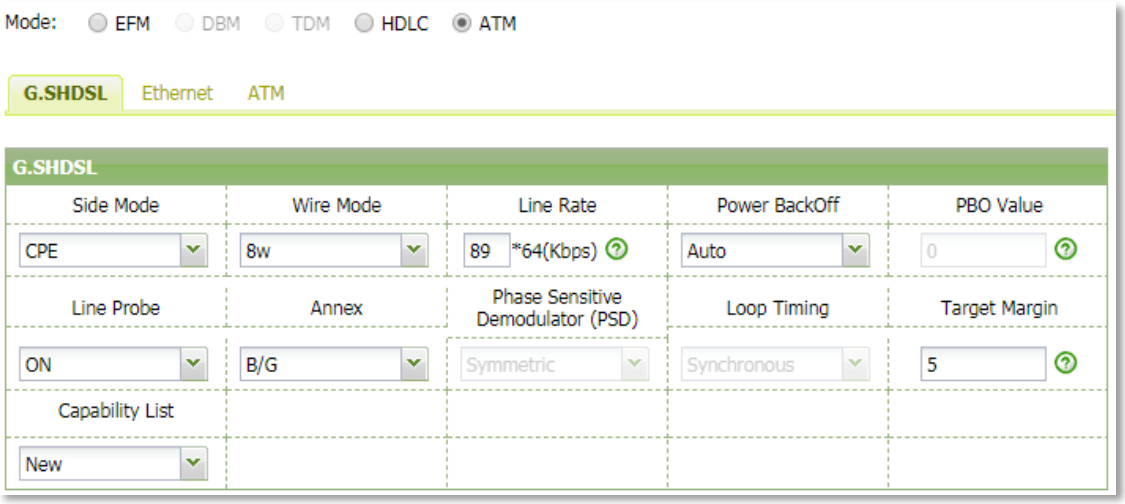


Figure 5-76 CPE-VLAN

2. Configuration > Local Setting > ATM

All settings are same as "**CO**".

Index 2: VID=**10** / VPI=**7** / VCI=**2000**

3. Configuration > General Setup > Local

Figure 5-77 CPE-General Setup

4. Bridge / Routing > VLAN

All settings are same as CO.

VLAN Rule= **Tag-based** / DSL, CVID=**10**

Tag a **VLAN 1** on DSL

Tag a **VLAN 10** on LAN-2 & DSL

Note:
After the modems are being connected, data will pass through the DSL about 10 ~ 30 seconds later. Do not forget to save in the end.

5.10.2 VLAN Application

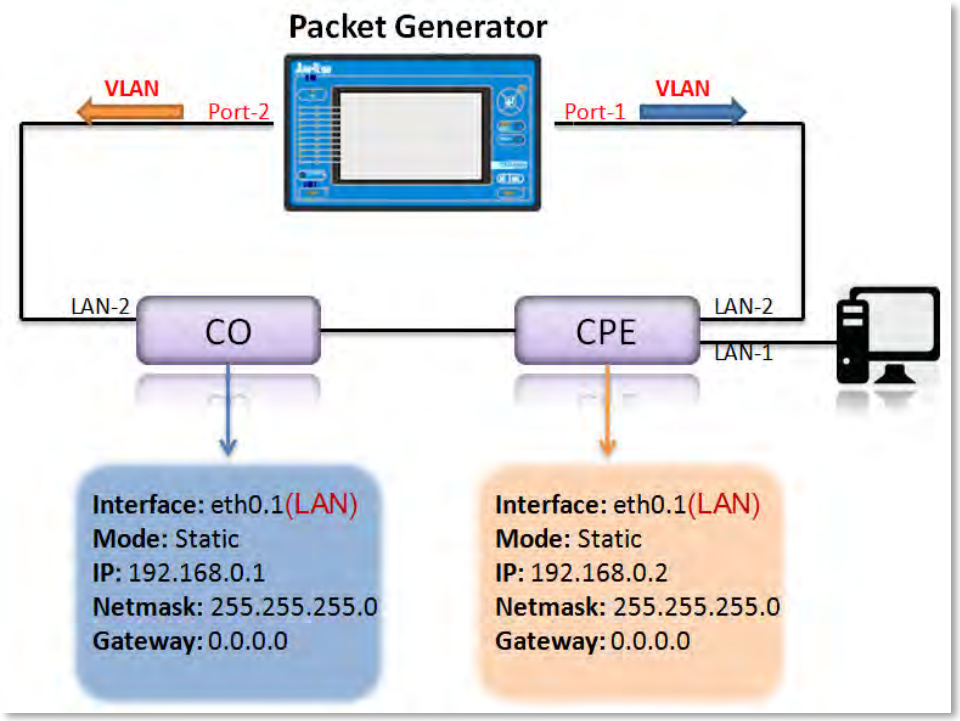


Figure 5-78 VLAN Application

- < CO configuration >

  Configuration > Local Setting > G.SHDSL

  Switch the dip switch on or change the device mode to "**CO**".

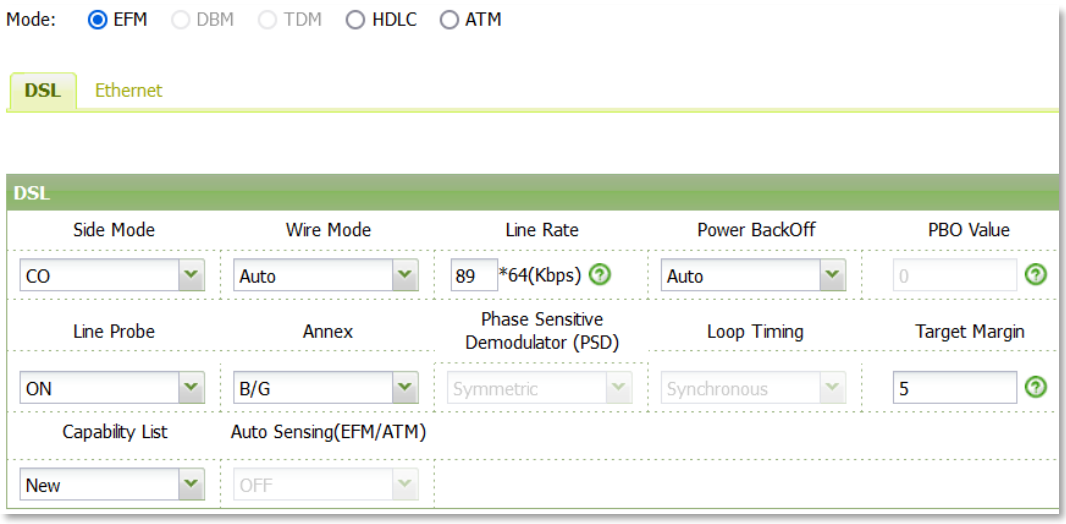


Figure 5-79 CO-G.SHDSL

- < CPE configuration >

  1. Configuration > Local Setting > G.SHDSL

     The default master-slave relationship of Comet 1608F is "**CPE**".

  2. Configuration > General Setup > Local

Figure 5-80 CPE-General Setup

  3. Bridge / Routing > VLAN

     VLAN Rule= **Tag-based**

- Tag-based mode is defined as CVID (Egress), for comparing with VLAN table.
- Add VLAN in the form and configure different VLAN function on all ports. Below is one of our examples.

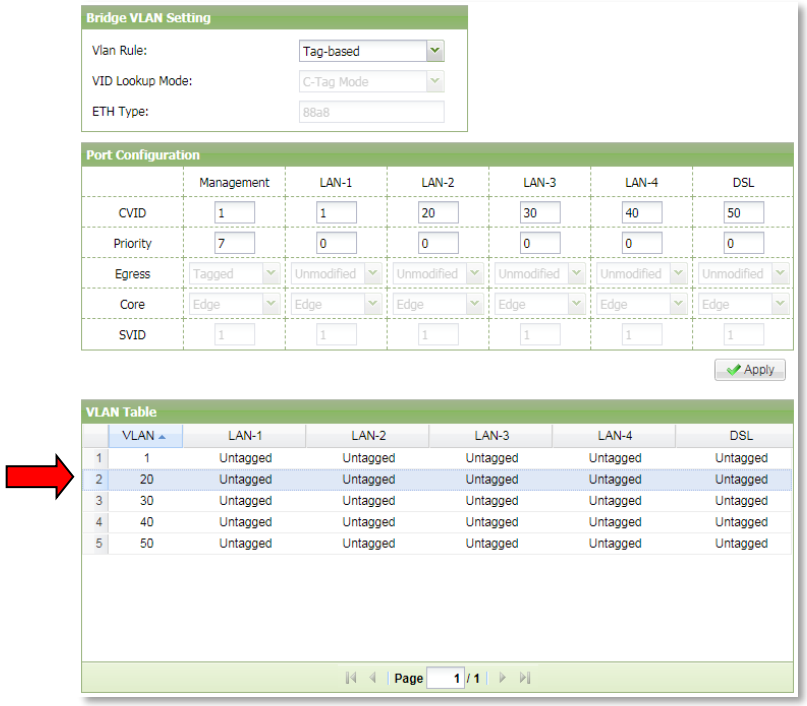


Figure 5-81 CPE-VLAN

** Notes: Remember to save after configured.

Test Result:

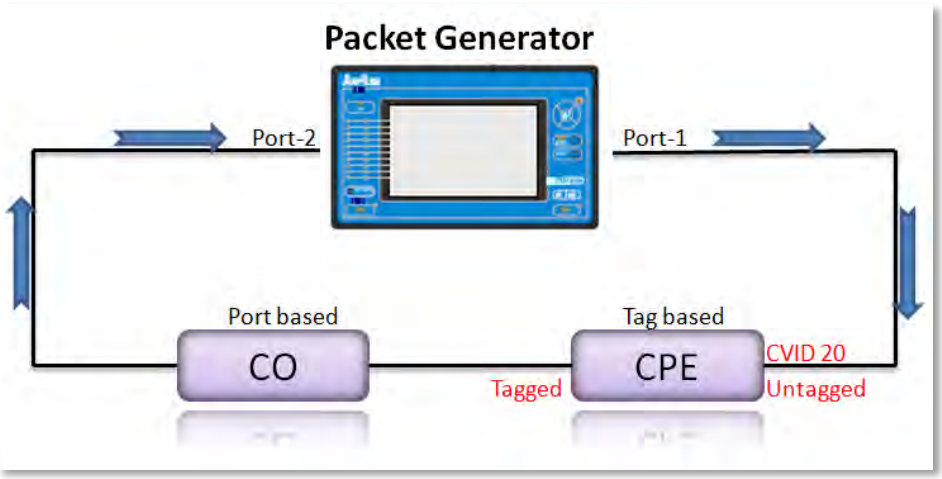


Figure 5-82 VLAN Test Result - 1

Data Direction: Port 1 --> Port 2	
Port 1	**Port 2**
Untagged	81000014
Tagged 20 (81000014)	81000014
Tagged 100 (81000064)	**X**

Table 5-4 VLAN Test Result - 1

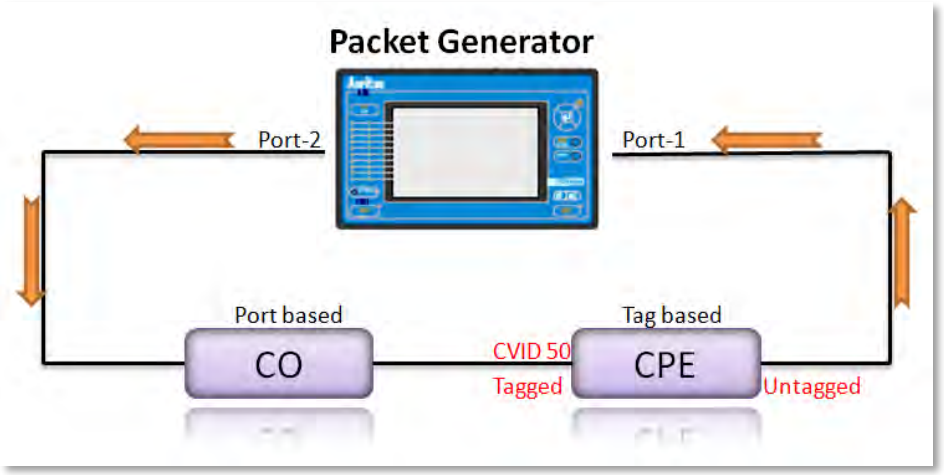


Figure 5-83 VLAN Test Result – 2

Data Direction: Port 2 --> Port 1	
Port 2	**Port 1**
Untagged	Untagged
Tagged 50 (81000032)	Untagged
Tagged 100 (81000064)	**X**

Table 5-5 VLAN Test Result - 2

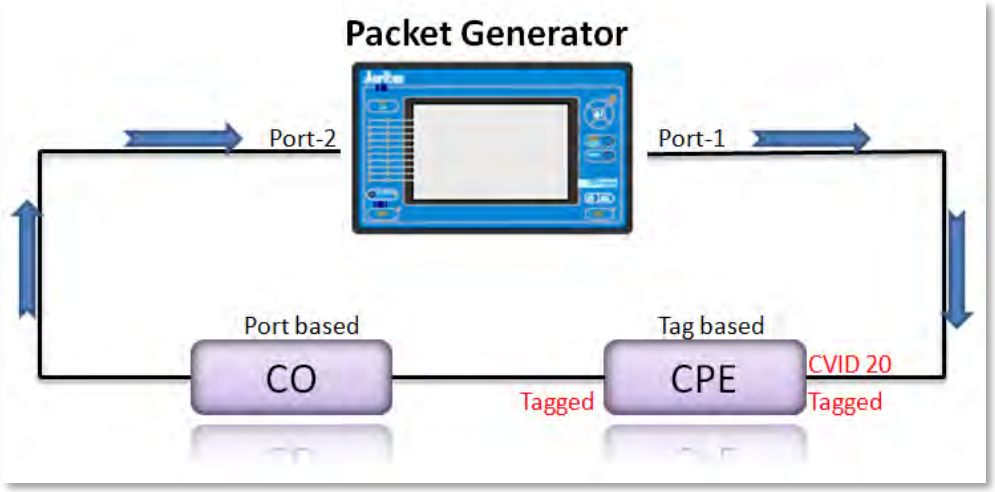


Figure 5-84 VLAN Test Result – 3

Data Direction: Port 1 --> Port 2	
Port 1	**Port 2**
Untagged	81000014
Tagged 20 (81000014)	81000014
Tagged 100 (81000064)	**X**

Table 5-6 VLAN Test Result - 3

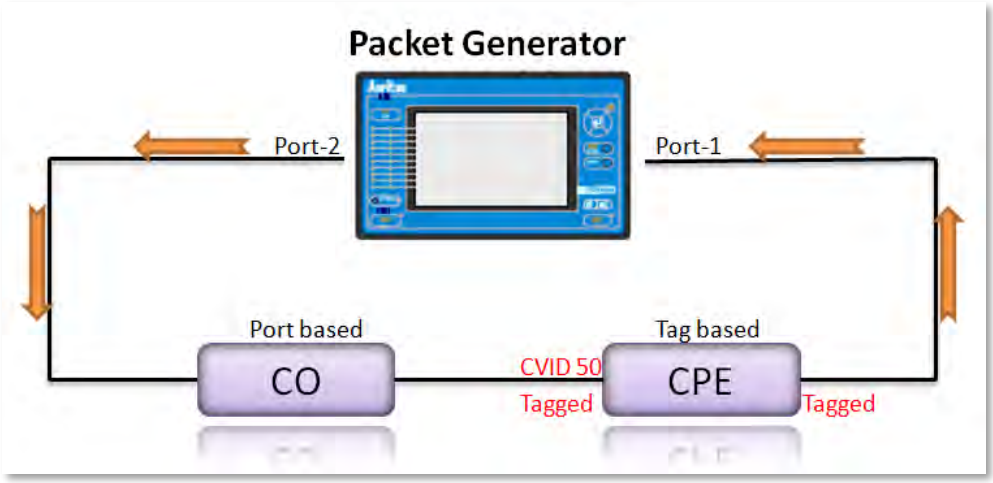


Figure 5-85 VLAN Test Result – 4

Data Direction: Port 2 --> Port 1	
Port 2	**Port 1**
Untagged	81000032
Tagged 50 (81000032)	81000032
Tagged 100 (81000064)	**X**

Table 5-7 VLAN Test Result - 4

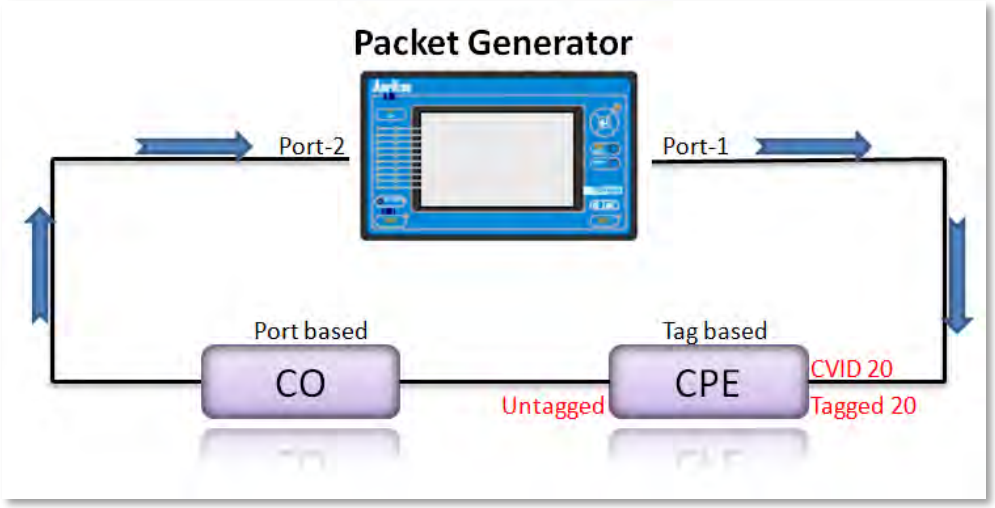


Figure 5-86 VLAN Test Result – 5

Data Direction: Port 1 --> Port 2	
Port 1	**Port 2**
Untagged	Untagged
Tagged 20 (81000014)	Untagged
Tagged 100 (81000064)	**X**

Table 5-8 VLAN Test Result – 5

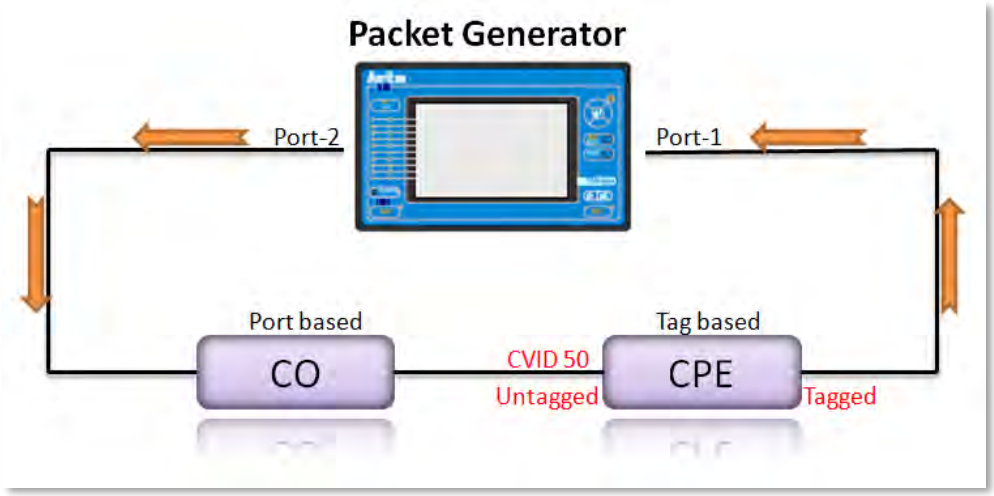


Figure 5-87 VLAN Test Result – 6

Data Direction: Port 2 --> Port 1	
Port 2	**Port 1**
Untagged	81000032
Tagged 50 (81000032)	81000032
Tagged 100 (81000064)	**X**

Table 5-9 VLAN Test Result - 6

5.10.3 Basic Routing

Routing Application:

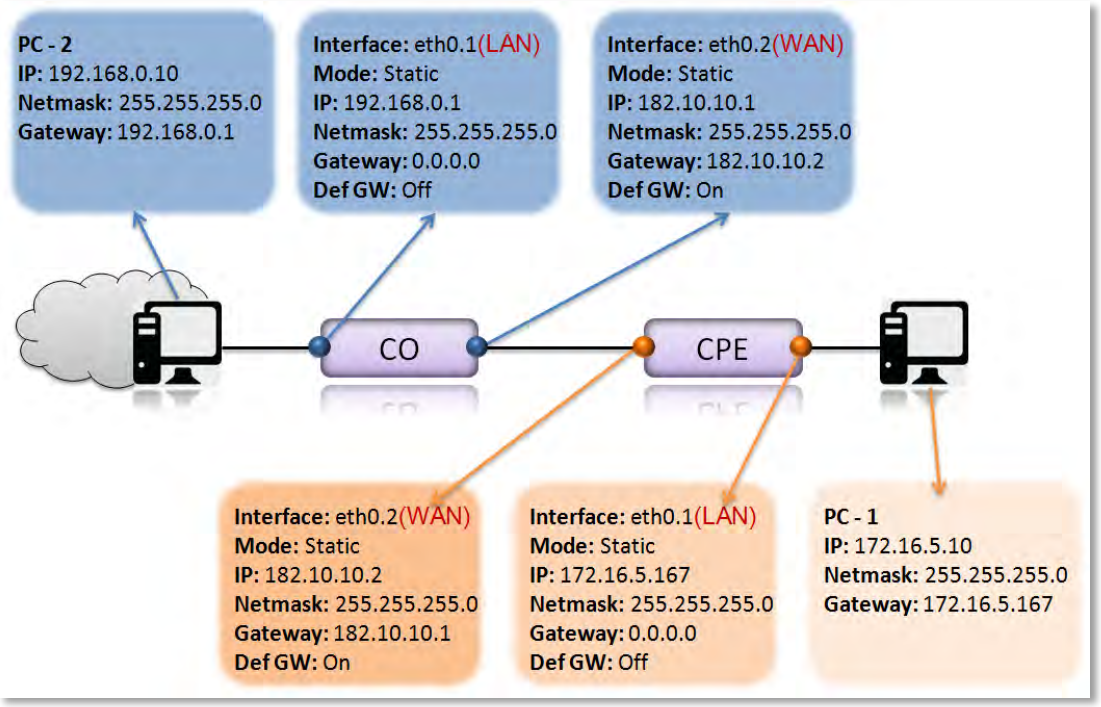


Figure 5-88 Routing Application

- < CO configuration >

1. Configuration > Local Setting > G.SHDSL

Switch the dip switch on or change the device mode to "**CO**".

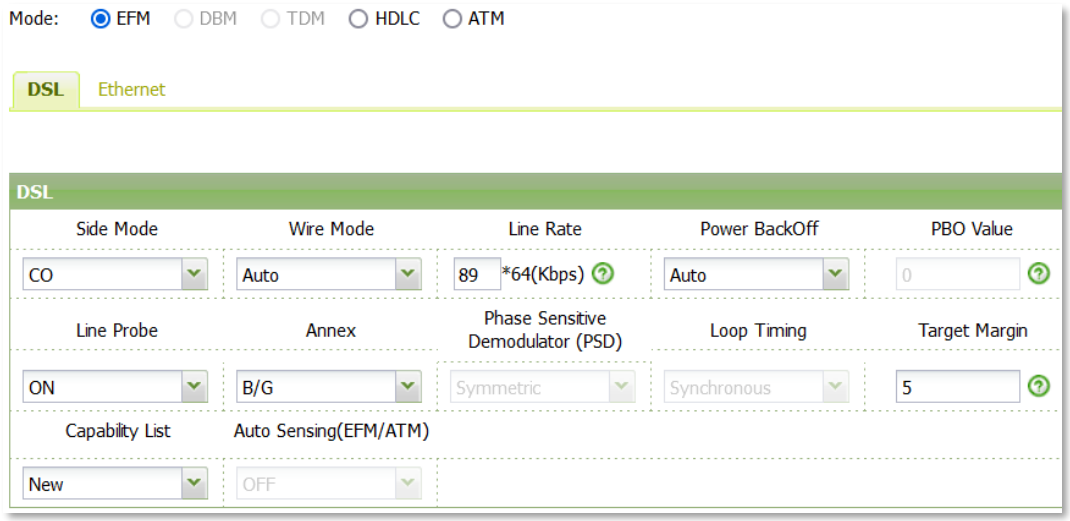


Figure 5-89 CO-G.SHDSL

2. Bridge / Routing > VLAN

Ex. VLAN Rule= **Tag-based** / DSL, CVID= **2**

All ports with **VLAN 2** are **untagged** for acting WAN.

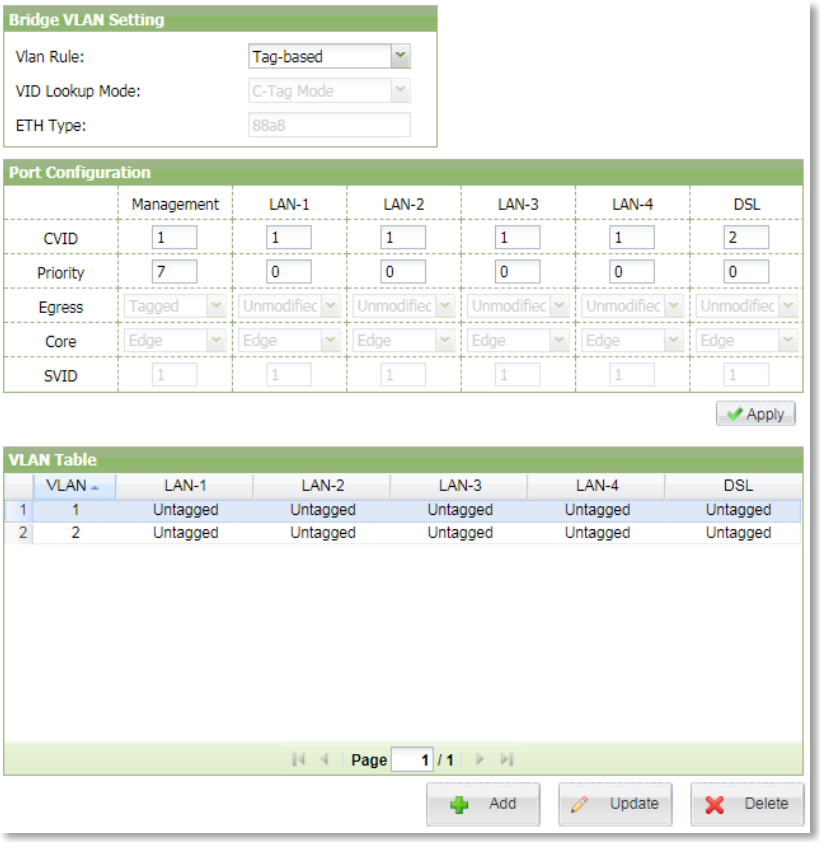


Figure 5-90 CO-VLAN

3. Bridge / Routing > Virtual IP

Add & Update all Virtual IPs, **eth0.1** acts as LAN and **eth0.2** acts as WAN.

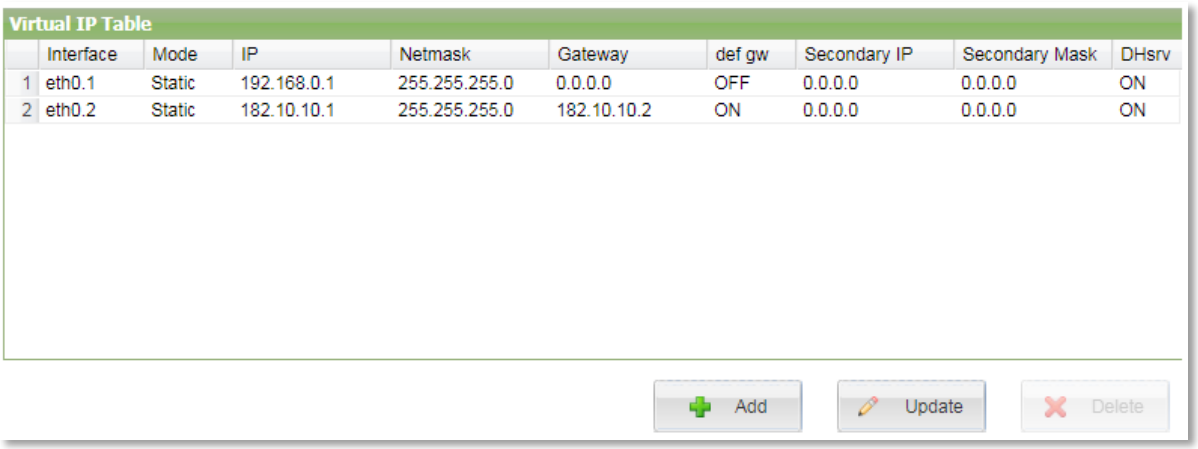


Figure 5-91 CO-Virtual IP

** Notes: Remember to save after configured.

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

The default master-slave relationship of Comet 1608F is "**CPE**".

2. Bridge / Routing > VLAN

All settings are same as "**CO**".

3. Bridge / Routing > Virtual IP

Add & Update all Virtual IPs, **eth0.1** acts as LAN and **eth0.2** acts as WAN.

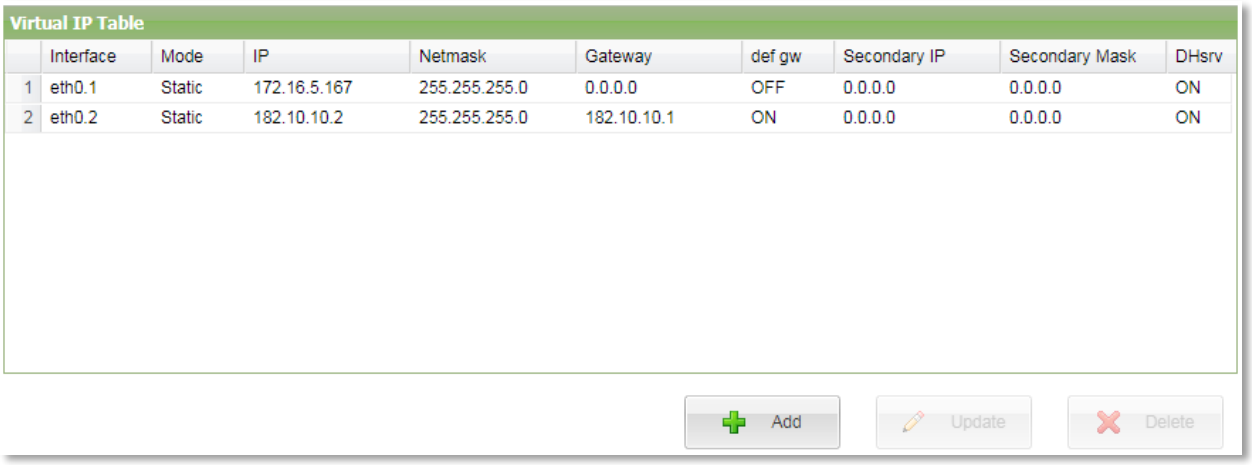


Figure 5-92 CPE-Virtual IP

** Notes: Remember to save after configured.

5.10.4 NAT Routing Application

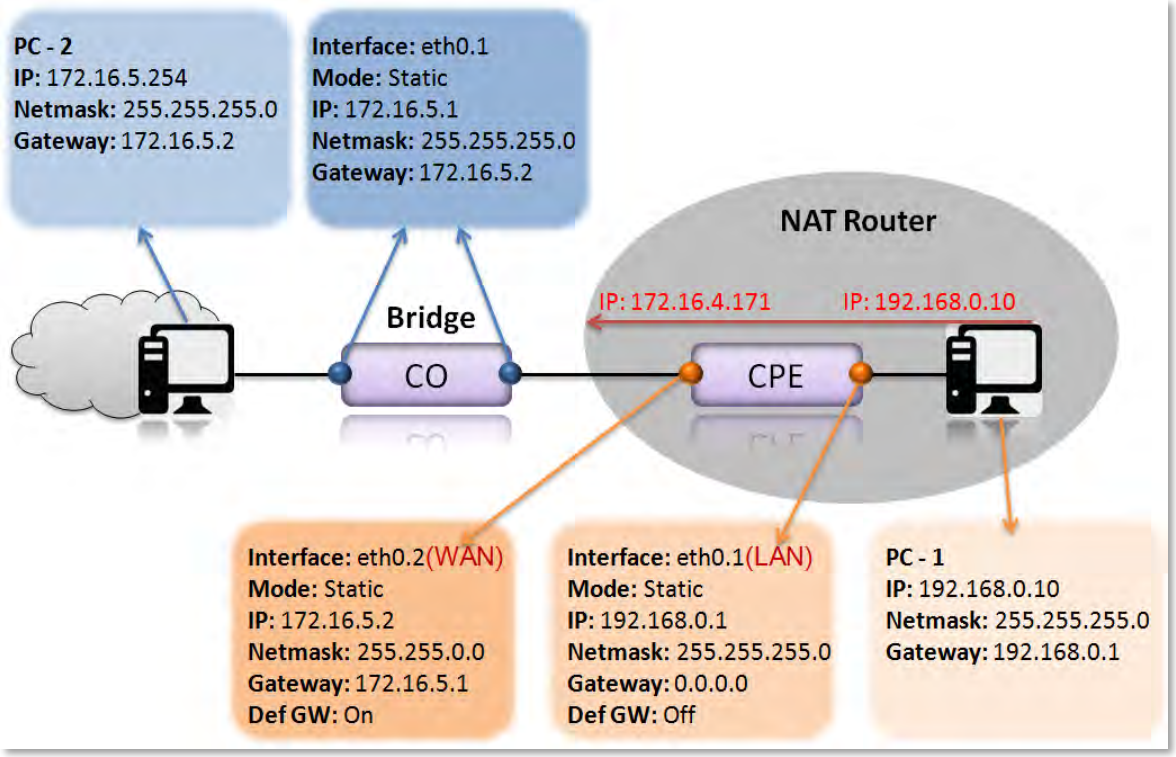


Figure 5-93 NAT Routing Application

- < CO configuration >

  1. Configuration > Local Setting > G.SHDSL

  Switch the dip switch on or change the device mode to "**CO**".

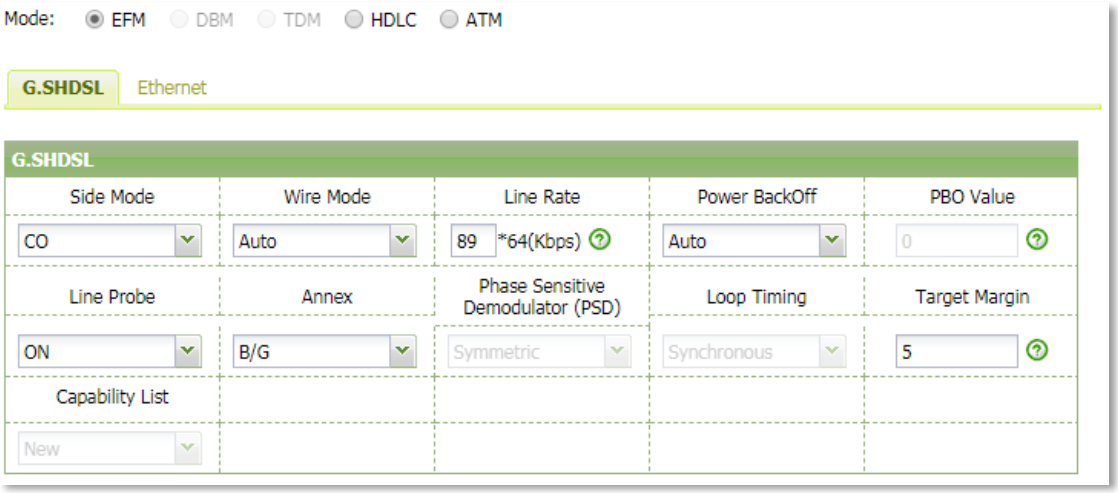


Figure 5-94 CO-G.SHDSL

2. Configuration > General Setup > Local

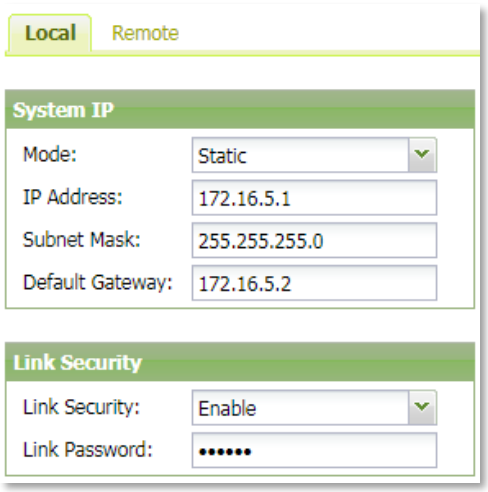


Figure 5-95 CO-General Setup

** Notes: Remember to save after configured.

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

The default master-slave relationship of Comet 1608F is "**CPE**".

2. Bridge / Routing > VLAN

Ex. VLAN Rule= **Tag-based** / DSL, CVID= **2**

All ports with **VLAN 1** are **untagged**.

All ports with **VLAN 2** are **untagged**.

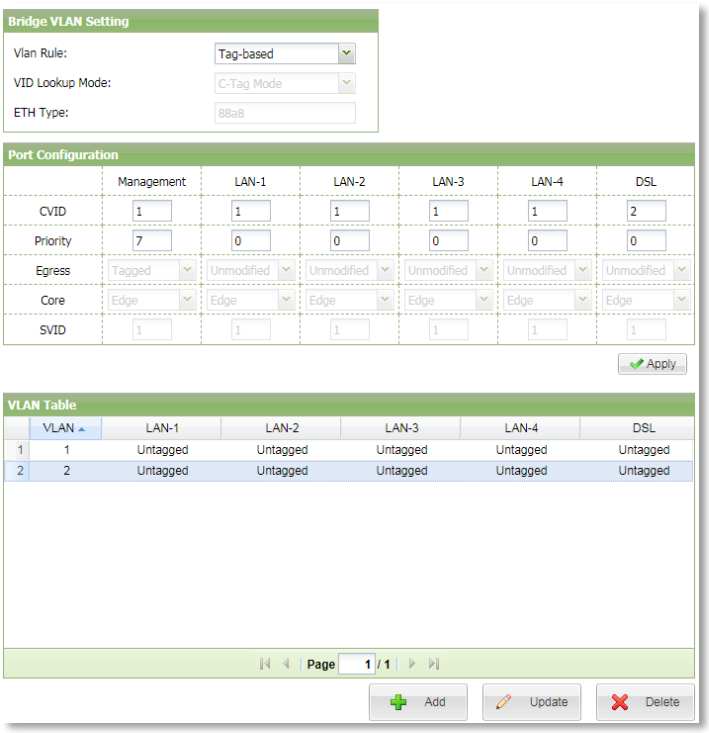


Figure 5-96 CPE-VLAN

3. Bridge / Routing > Virtual IP

Add & Update all Virtual IPs, **eth0.1** acts as LAN and **eth0.2** acts as WAN.

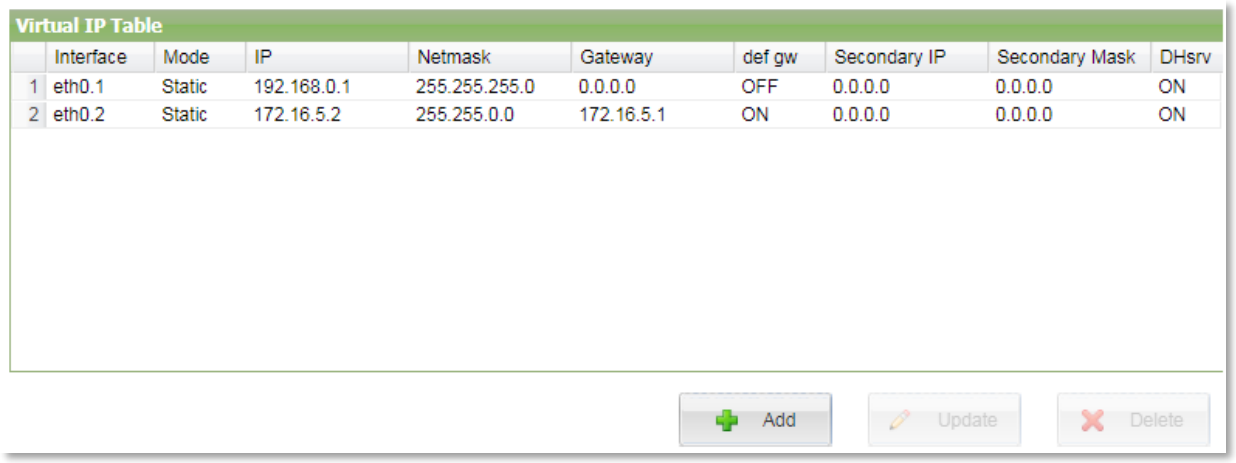


Figure 5-97 CPE-Virtual IP

4. Bridge / Routing > NAT table

Remap the source **IP(192.168.0.10)** into another **IP(172.16.4.10)** while packets are in transit across a traffic routing device for hiding themselves.

Source IP: **192.168.0.10** / **32**

Destination IP: **172.16.0.0** / **16**

Translation: **SNAT** / **POSTROUTING** / Line= **1** / Protocol= **ALL**

Start IP & End IP are **172.16.4.10** / Outface: **eth0.2**

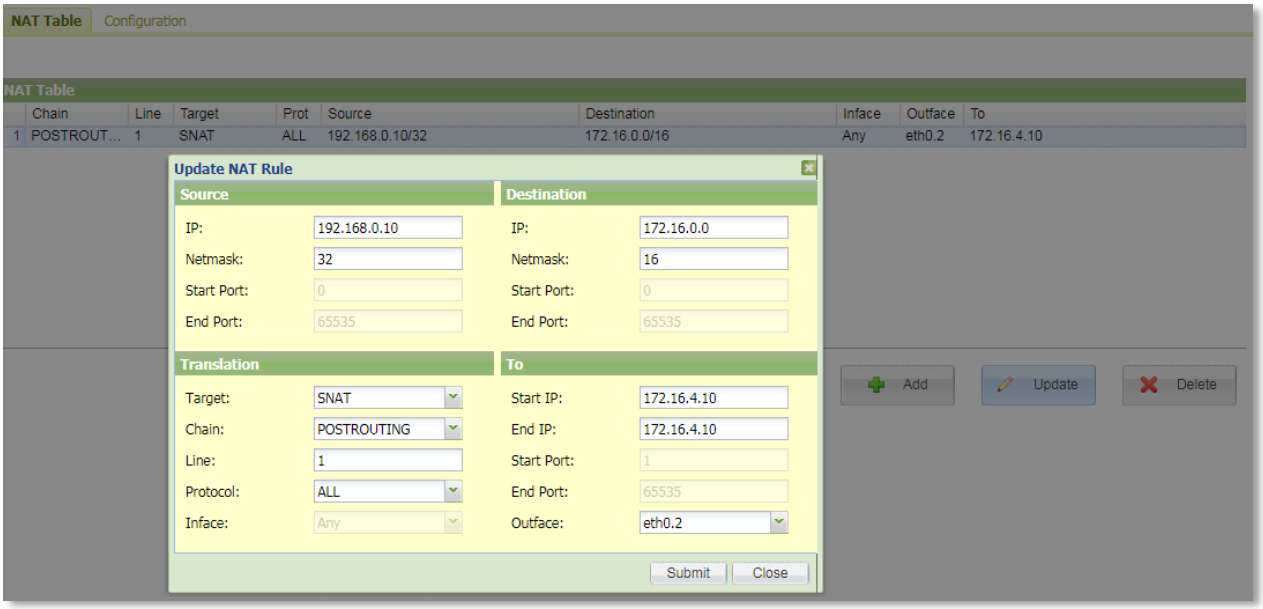


Figure 5-98 CPE-NAT Table

** Notes: Remember to save after configured.

5.10.5 VALN Multiplexer Application

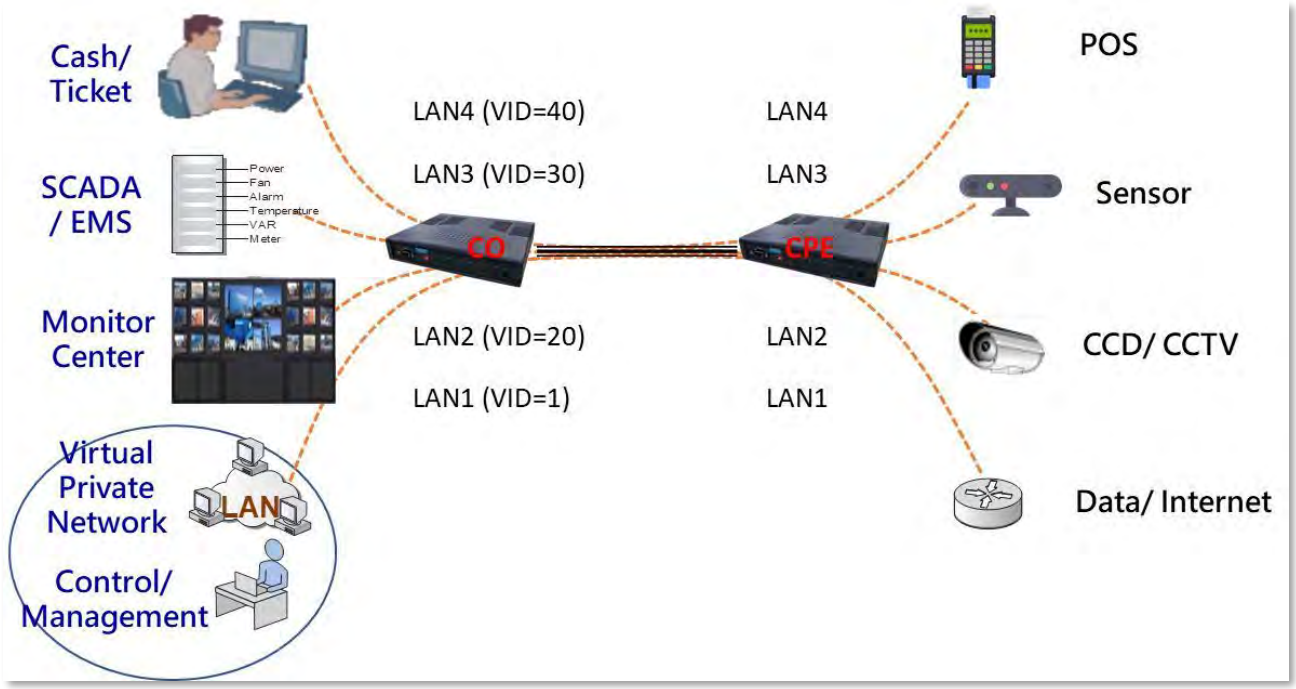


Figure 5-99 VLAN multiplexer application

Application:

Use G.SHDSL as long distance Ethernet Bridge that separates four different applications by different LAN port connection. Each LAN port has their own traffics which isolated from other LAN ports.

Configuration:

Control/ Management PC IP address: 192.168.0.170

Comet at CO IP address: 192.168.0.108

Comet at CPE IP address: 192.168.0.109

Default Login Username: admin

Default Login Password: admin

Comet default IP address: 192.168.0.1

1. To simplify the configuration, all configurations begin with loading the factory default: [Maintenance]→[Software Default]→[Apply]

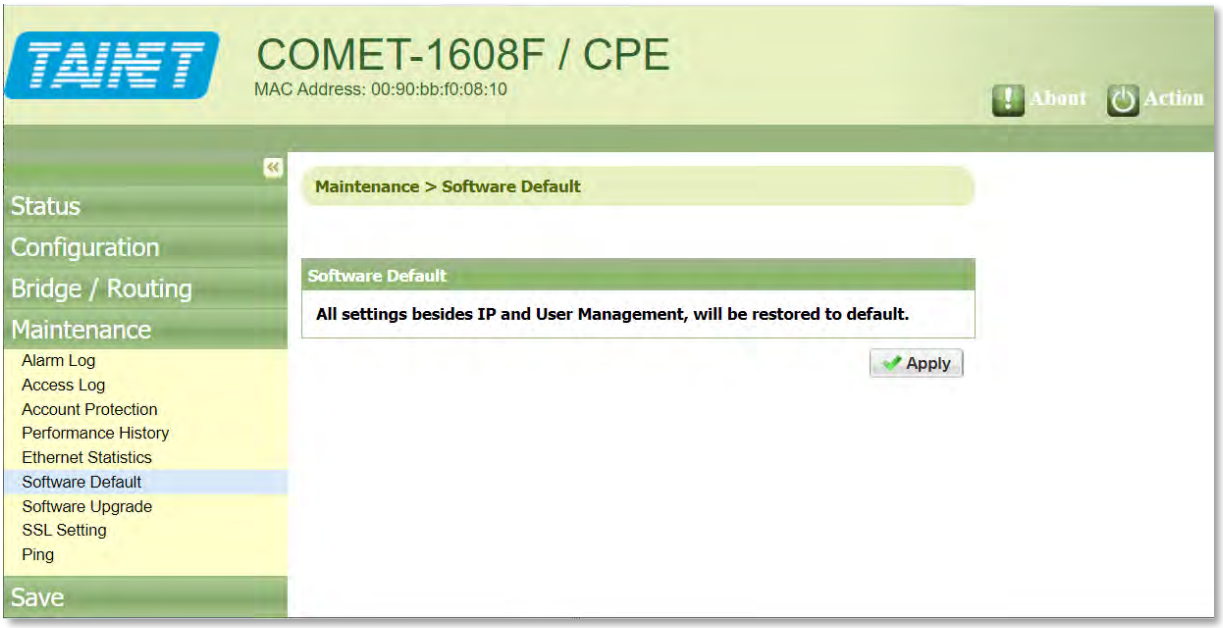


Figure 5-100 Restore to software default

2. On CPE site, [Configuration]→[Load Local Profile]→1.CPE →[Apply]

3. On CO site, [Configuration]→[Load Local Profile]→2.CO →[Apply]

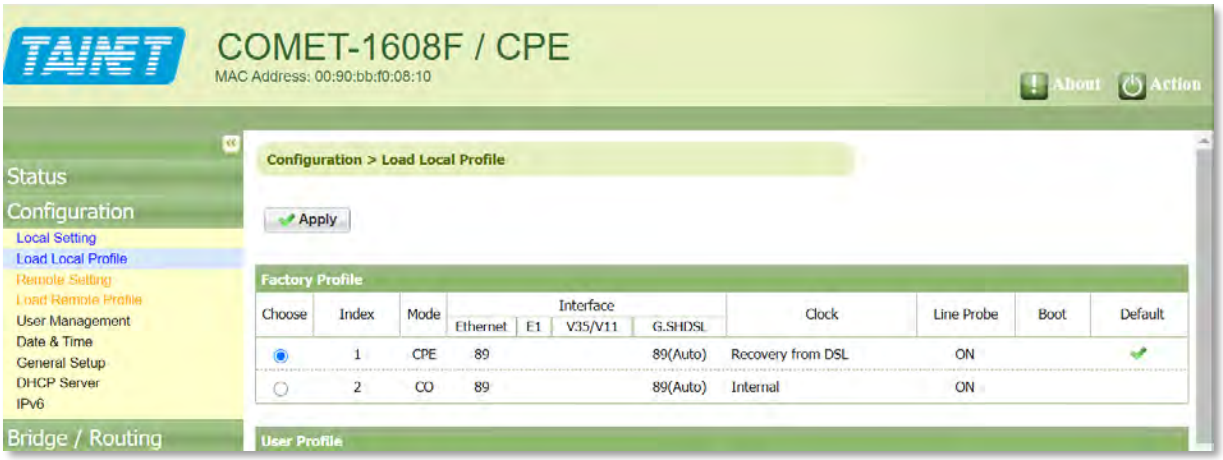


Figure 5-101 Load factory CPE default profile

4. CO site change IP address to 192.168.0.108
   [Configuration]→[General Setup]→Local [System IP] →[IP address] →192.168.0.108

Figure 5-102 Change IP address of CO device

5. CPE site change IP address to 192.168.0.109
   [Configuration]→[General Setup]→Local [System IP] →[IP address] →192.168.0.109

Figure 5-103 Change IP address of CPE device

6. Change the VLAN Rule to [Tag-based] in Bridge/ Routing group.
   [Bridge/ Routing] → [VLAN] → [VLAN Rule] → Tag-based → [Apply]

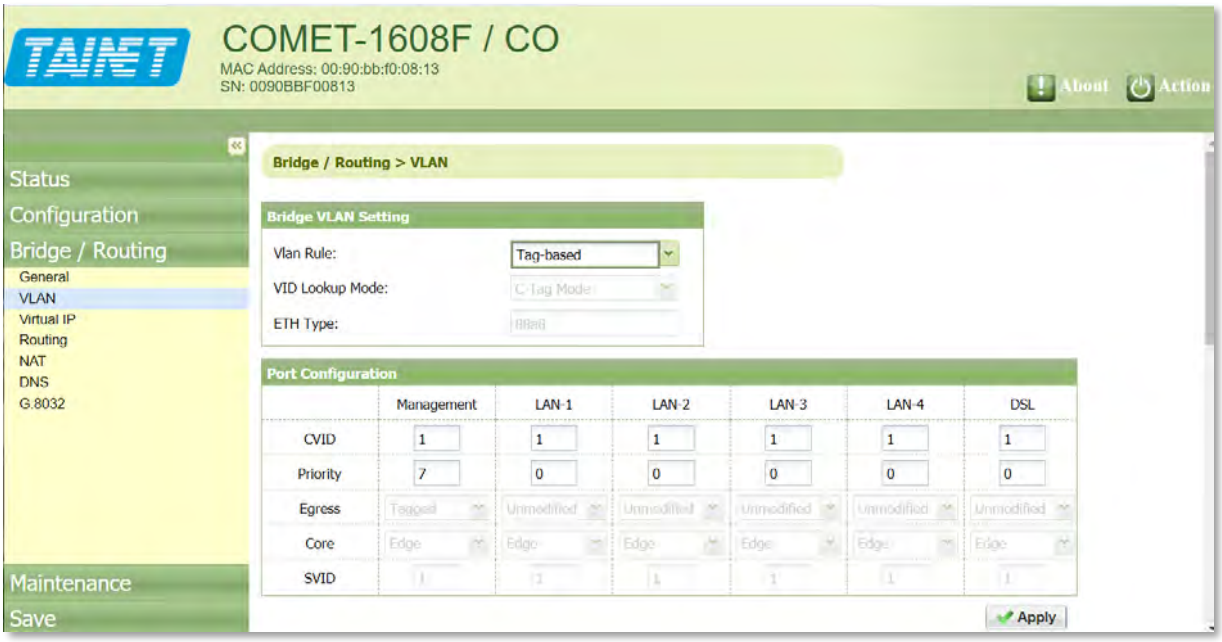


Figure 5-104 Apply Tag-based VLAN rule

7. Edit VLAN table, the VLAN table will show after Tag-based rule has been selected.
   [Bridge/ Routing] → [VLAN] →[VLAN Table]→1 →[Update]

Figure 5-105 Setup VLAN Table configuration

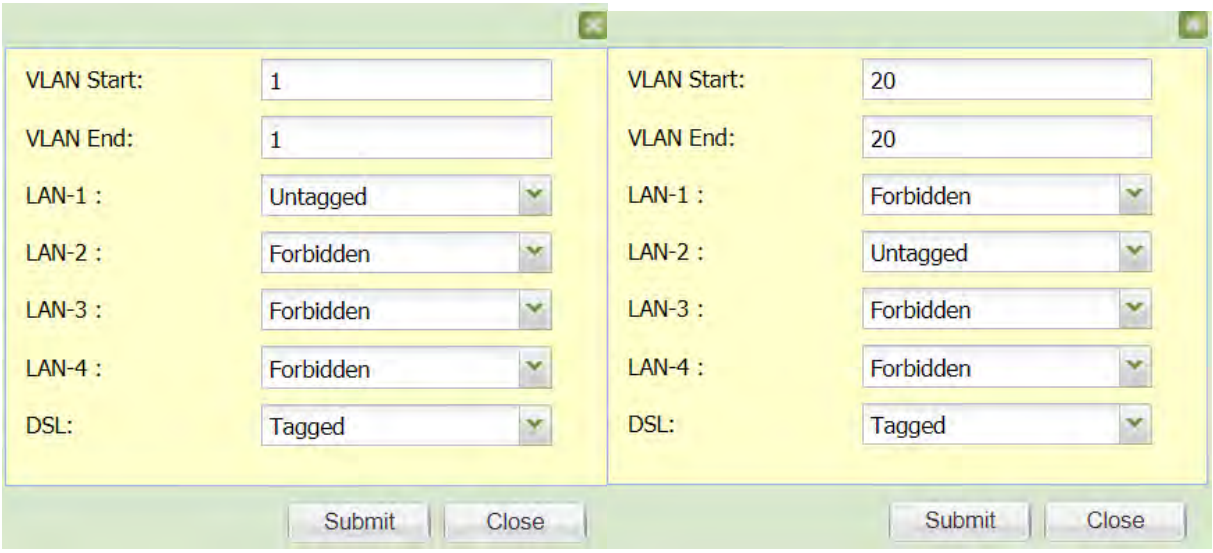


Figure 5-106 Setup VLAN rule of VID 1 and 20

[Bridge/ Routing] → [VLAN] →[VLAN Table] →[Add]→20

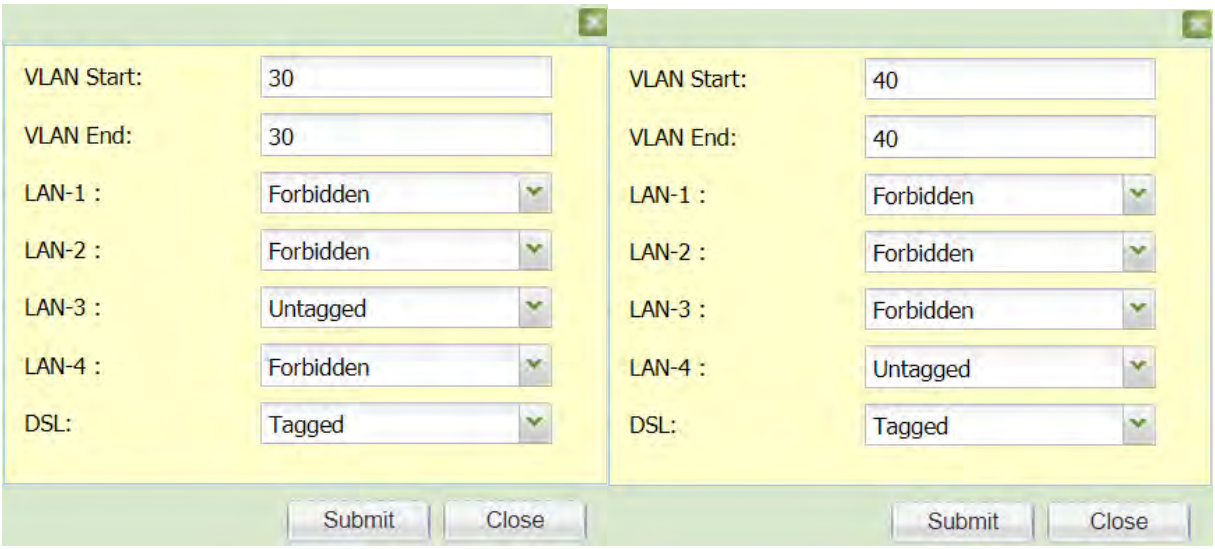
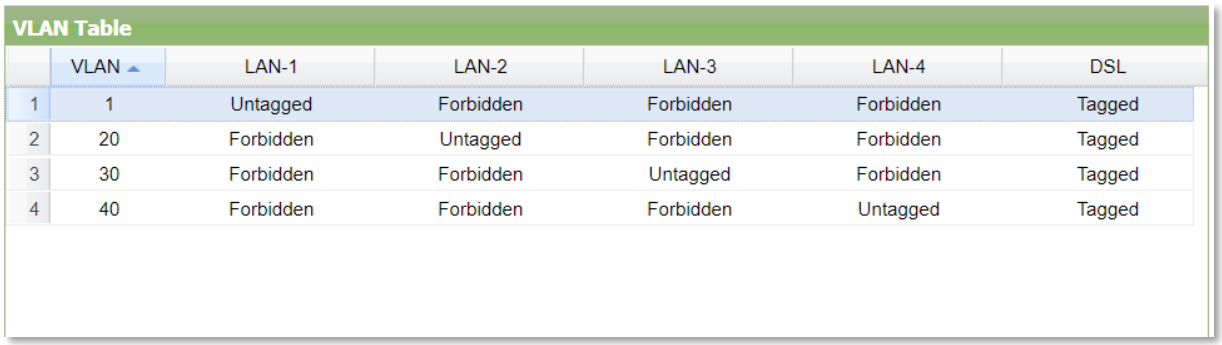


Figure 5-107 Setup VLAN rule of VID 30 and 40

[Bridge/ Routing] → [VLAN] →[VLAN Table] →[Add]→30
[Bridge/ Routing] → [VLAN] →[VLAN Table] →[Add]→40



VLAN Table

	VLAN	LAN-1	LAN-2	LAN-3	LAN-4	DSL
1	1	Untagged	Forbidden	Forbidden	Forbidden	Tagged
2	20	Forbidden	Untagged	Forbidden	Forbidden	Tagged
3	30	Forbidden	Forbidden	Untagged	Forbidden	Tagged
4	40	Forbidden	Forbidden	Forbidden	Untagged	Tagged

Figure 5-108 Applied list of VLAN Table

8. Edit VLAN Table → Port Configuration → CVID
   [Bridge/Routing] → [VLAN] → Port Configuration [CVID] → 1, 1, 20, 30, 40, 1 →[Apply]

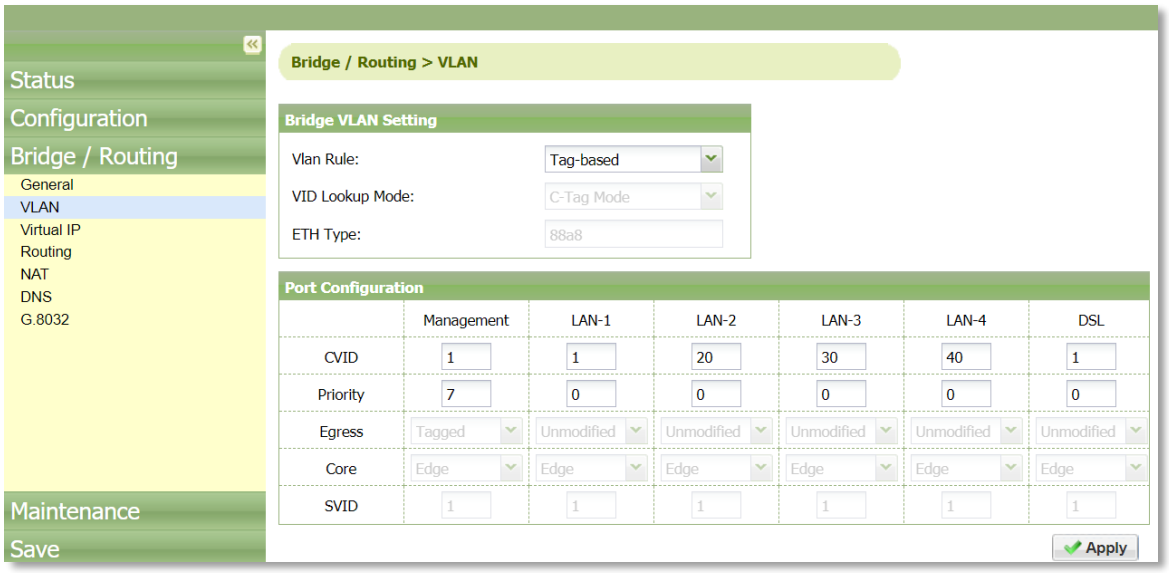


Figure 5-109 Setup the Core port VID

9. [Save]→[Local Save]→SHDSL→[OK]

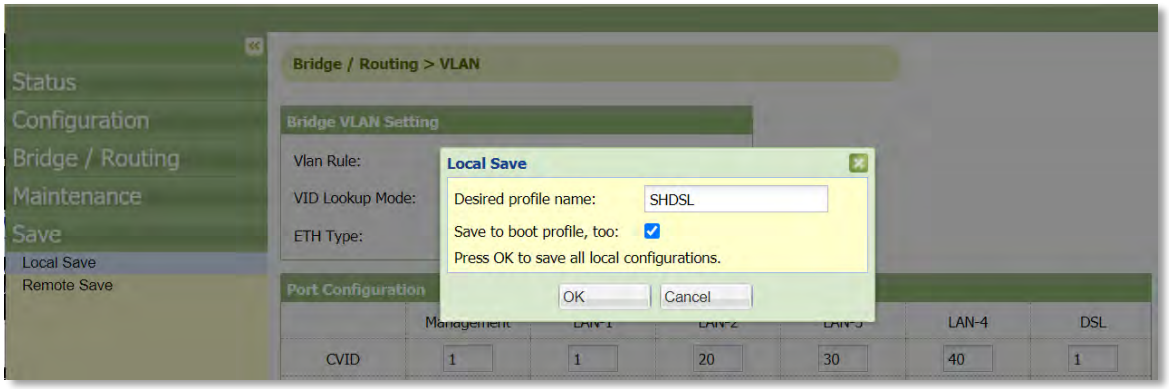


Figure 5-110 Save the working configuration to profile

10. Do the same procedure from steps 6 to 9 on CPE to complete the whole configuration.

Notice:

1. Must follows step by step order form 6, 7 to 8th; change the order may cause the loss of management control. Should be carefully.
2. The default username and password are easily be hacked, do remember to change it with more complexity when formal deployed.
3. Change the VLAN Rule to [Tag-based] in Bridge/ Routing group will also change the System IP setting from Configuration/[General Setup] to Bridge/ Routing [Virtual IP].

Chapter 6. Operator of CID

This Chapter describes the Terminal User Interface provided by Comet 16xxF/160xFM. There are two methods to access to the Terminal User Interface: The Craft port and Telnet, those present the exact same format of terminal management. The Craft port is used primarily when the device is installed for the first time and the IP configuration is not yet provisioned. Once when the IP connection is provisioned, users may login to the Terminal User Interface by using the Telnet software to remotely control or maintain the device from anywhere in the global IP network. The following introductions are based on the Comet 1608F with firmware code **v1.430**.

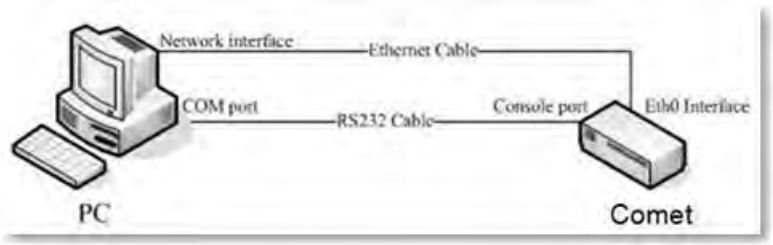


Figure 6-1 Basic Management Connection

6.1 The connection via Craft Port

By using the VT-100/ANSI compatible terminal emulation software, such as Microsoft HyperTerminal or Tera Term, users can configure Comet 160xF/ FM and 160xF-R/ FM-R via the Craft port with console cable.

Select the COM port used and setup the following settings:

- Speed: **115200 bps** (bit per second)
- Date Length: **8 bits**
- Parity Bit: **None**
- Stop Bit: **1 bit**
- Flow Control: **None**

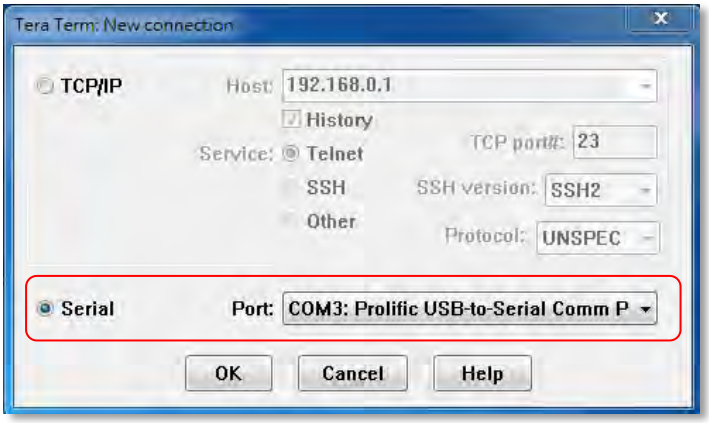


Figure 6-2 Select the correct Series Port in Tera Term

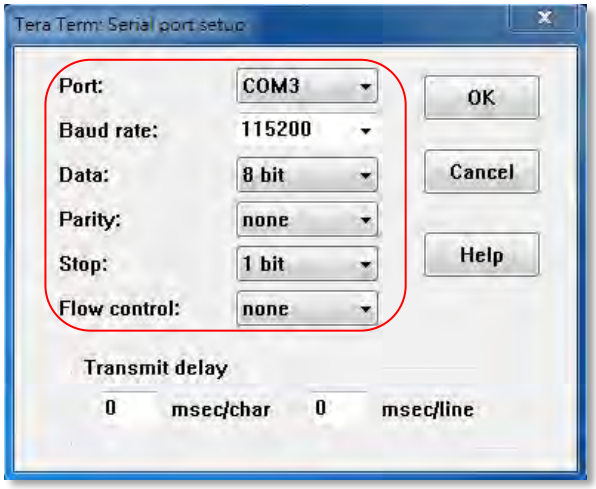


Figure 6-3 Series Port Parameters

6.2 The connection via Telnet/SSH Protocol

Below is the default IP address of Comet 160xF/ FM, users input the correct IP address to access the device by Telnet and SSH protocol.

Default IP address: 192.168.0.1

Default gateway: 192.168.0.254

Default netmask: 255.255.255.0

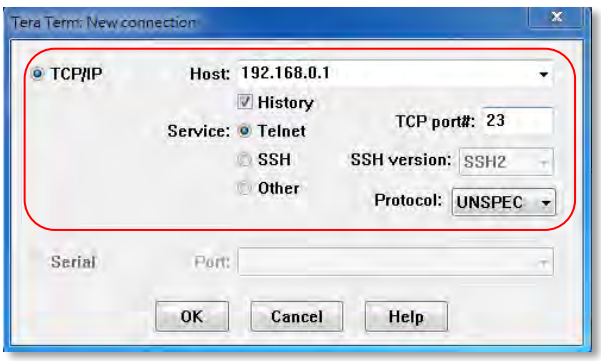


Figure 6-4 Select Telnet/ SSH with correct IP

6.3 The Command Line Interface

When the security authority is passed, the terminal UI will display the Root Menu as shown in the following, user has to input correct account and password for the login process. The default highest authority is admin/admin.

Figure 6-5 Login Screen of TAINET

After log in the system, input the command "**help**" or "**?**" to display main command lines. Press any key on keyboard to display complete items.

Figure 6-6 Main Command Lines

6.3.1 "aclset" Command

The command is used to set ACL, Comet supports two methods, "**normal**" and "**white list**" with different match conditions will filtered specified data packages. TAINET prepare many detailed examples for users' references.

```
LOCAL >aclset

---------- CLI_ACL_SET_Help ---------------
 Usage   : Set ACL Configuration/Rules
 Synopsis:
    acls [options] [value]
 ============================================
options:
        -y   Select ACL mode [1: normal, 2:white list]
        -N   Delete ACL rule entry[1~40]
        -t   Ingress port bitmap(hex) , no use bit is 0
        -x   Egress port bitmap(hex) , no use bit is 0
                 [ 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:DSL]
        -f   Frame type [0:Mac, 1:IPv4, 2:IPV4+L4Port, 3:L4Port]
 --------------------------------------------
MAC Type ==>

        -d   DMAC [xx:xx:xx:xx:xx:xx]
        -n   DMAC mask [xx:xx:xx:xx:xx:xx]
        -s   SMAC [xx:xx:xx:xx:xx:xx]
        -m   SMAC mask [xx:xx:xx:xx:xx:xx]
        -e   EtherType value [xxxx(hex)]
        -k   EtherType mask [xxxx(hex)]
IPv4 Type ==>

        -i   DIP(IPv4)
        -n   DIP(IPv4) mask
        -s   SIP(IPv4)
        -m   SIP(IPv4) mask
IPv4+L4Port Type==>  only available in white-list mode

        -s   SIP(IPv4)
        -m   SIP(IPv4) mask
        -p   TCP/UDP Destination port [0~65535]
        -k   TCP/UDP Destination port mask [xxxx(hex)]
L4Port Type(white list) ==>

        -p   TCP/UDP Destination port(start) [0~65535]
        -q   TCP/UDP Destination port(end) [0~65535]
L4Port Type(normal) ==>

        -p   TCP/UDP Destination port [0~65535]
        -k   TCP/UDP Destination port mask [xxxx(hex)]
```

Figure 6-7 "aclset" Command

6.3.2 "aclget" Command

Input this command to get ACL rules.

```
LOCAL >aclget
|-------------------------------------------------------------------------|
|Index|        ACL Mode|       Frame Type|             SIP|         SIP Mask|
|-----|----------------|-----------------|----------------|-----------------|
|    1|      White list|             IPv4|  192.168.  0. 21|  255.255.255.255|
```

Figure 6-8 "aclget" Command

6.3.3 "arp" Command

Input this command to get matches IP and VLAN.

```
LOCAL >arp

---------- CLI_ARP_Help ---------------
Usage   : ARP Table Operation
Synopsis: arp [Option]
============================================

Option  :
  -a/n   show Full ARP Table
  -i     show ARP Entry that matches IP
  -v     show ARP Entry that matches VLAN

Example :
  1. Show ARP Entry that matches both IP (216.239.35.12) and VLAN (1)
     arp -i 216.239.35.12 -v 1
```

Figure 6-9 "arp" Command

6.3.4 "atmset" Command

The command is used to set ATM function, only the G.SHDSL mode is ATM can be configured by "atmset".

```
LOCAL >atmset

argc can't equal to 1,2, and >9.

Usage: Setup ATM parameter !
SYNOPSIS: atmset [options] [value]
options:
        -s  [ CPCS Protocol ]  '1':VC_MUX_BP, '2':LLC_ENCAP_BP
        -f  [Filter Mode] '1': vlan ID
        -a  [Default Action]  '1':discard, '2':default VPI/VCI
     -m  modify filter table index (1~4)
     -d  Default value
        -v  [ VLAN ID ]  set  ( 1~ 4095 )  value
        -p  [ VPI ]  set  ( 0~255 )  value
        -c  [ VCI ]  set  ( 32~2000 )  value
Example:  atmset -s 2 -a 2
Example:  Modify index:1 VID, VPI or VCI in filter table
Example:  atmset -m 1 -v 2 -p 5
Example:  atmset -m 1 -v 2 -p 5 -c 35
Example:  Set default VPI or VCI
Example:  atmset -d -p 0
Example:  atmset -d -p 0 -c 35
```

Figure 6-10 "atmset" Command

6.3.5 "atmget" Command

The command is used to check ATM function, such as CPCS Protocol, VID, VPI and VCI.

```
LOCAL >atmget
CPCS Protocol :  LLC_ENCAP_BP
Filter Mode :  VLAN ID
Default Action :  default VPI/VCI
Filter Table
----------|--------|--------|--------
Index     |VID     |VPI     |VCI
----------|--------|--------|--------
1         |1       |1       |35
----------|--------|--------|--------
2         |2       |2       |35
----------|--------|--------|--------
3         |3       |3       |35
----------|--------|--------|--------
4         |4       |4       |35
----------|--------|--------|--------
5         |5       |5       |35
----------|--------|--------|--------
6         |6       |6       |35
----------|--------|--------|--------
7         |7       |7       |35
----------|--------|--------|--------
8         |8       |8       |35
Default_VPI:0, VCI:35
```

Figure 6-11 "atmget" Command

6.3.6 "briget" Command

The command is one of the most important commands in routing application. Users are able to check VLAN rule and Port Info by "**–c**", Port Forwarding by "**-p**", MAC table by "**-m**" and VLAN table by "**-v**".

```
LOCAL >briget

---------- CLI_BridgeGet_Help ---------------
 Usage   : Get Bridge Information
 Synopsis:
    briget [Options]
 ============================================
 Options:
    -a          Show ALL below
    -c          Show Configuration
    -p          Show Port Forwarding Member
    -m          Show Mac Table
    -v          Show VLAN Table
    -n          Show VLAN Translation Table
```

Figure 6-12 "briget" Command

6.3.7 "briset" Command

The command is used to set VLAN function. There are three main VLAN rules, such as tag based, port based and Q-in-Q. TAINET prepares many examples for users' references in CLI mode.

- **Tag based → Routing mode**
- **Port based → Bridge mode**

```
LOCAL >briset

---------- CLI_Bridge_SET_Help --------------------
 Usage   : Set Bridge Configuration
 Synopsis:
   briset [Option][value]


 ============================================
 briset Options:
   -g    agingtime        1~65535(sec)
   -r    vlan-rule        [0]:tag-base [1]: port-base [2]QinQ
   -t    qos  type        [0]:802.1p [1]:tos/dscp [2]:port_priority
   -s    qos  schedule    [0]:wrr [1]:strict_priority
   -l    QinQ S-Tag Mode  [0]C-Tag Mode [1]S-Tag Mode
   -q    QinQ Eth type    [ffff] default: 88a8
   -k    QinQ SVID        [1~4094]
   -c    QinQ Core Port   [0]Edge Port [1]Core Port
   -p    port             [1~4]:eth1~4, [5]:DSL
   -i    port vid         [1~4094]
   -e    Egress Mode      [1]:Untagged [2]:Tagged [3]:Unmodified
   -o    port-base member mask (hex) , bit 0:Manag, 1~4:LAN-1~4, 5:DSL
   -m    mac_table
   -v    vlan_table
   -a    mac_table  add  port(1~2) MACaddress(xx:xx:xx:xx:xx:xx) or
   -a    vlan_table add vlanid(1~4094) lan1 lan2 dsl
         (lan1,lan2,dsl --> [0]:unmodified,[1]:untaged,[2]:tagged,[3]:forbidden)
   -d    mac_table  delete entry[1~8] or vlan_table delete entry[1~4094]
   -f    lan1/2 default priority value[0~7]
 ============================================
 Example(AgingTime and vlan Rule) : briset -g 300 -r 0
 Example(Qos type and schedule) : briset -t 3 -s 0
 Example(QinQ eth_type 88a8 S-Tag Mode) : briset -q 88a8 -l 1
 Example(QinQ port 1 SVID 4094 ) : briset -p 1 -k 4094
 Example(QinQ port 1 Edge Port ) : briset -p 1 -c 0
 Example(Port 1 port vid): briset -p 1 -i 3
 Example(Port 2 port vid): briset -p 2 -i 5
 Example(Mac table add port2 mac address):
       briset -m -a 2 xx:xx:xx:xx:xx:xx
 Example(Mac table delete entry 3 mac address) :
        briset -m -d 3
 Example(vlan table add vid:1 lan1:unmod lan2:unmod lan3:unmod lan4:unmod g.shdsl:unmod):
        briset -v -a 1 0 0 0 0 0
 Example(vlan table delete vlan 1 ):
        briset -v -d 1
 Example(set port 1 default priority value 1):
        briset -p 1 -f 1
 Example(set port 2 forward frame to LAN-1 and DSL ):
        briset -p 2 -o 22
 Example(set port 2 egress mode : Unmodified ):
        briset -p 2 -e 3
 Example(set DSL Core Port SVID 700 ):
        briset -p 5 -c 1 -k 700
```

Figure 6-13 "briset" Command

6.3.8 "communityset" Command

The command is used to set SNMPv2, such as security passwords of Agent Public Community, Agent Private Community and Trap Community.

```
LOCAL >communityset

Usage: Setup Community Password!
SYNOPSIS: communityset [-g,-s,-t] [password]
options:
        -g  Snmp Agent Public Community
        -s  Snmp Agent Private Community
        -t  Snmp Trap Community
        Password: [max -- 15]
Example:    communityset -g xxxxxxx
```

Figure 6-14 "communityset" Command

6.3.9 "communityget" Command

The command is used to get SNMPv2 information, only admin privilege can get SNMP Community information.

Figure 6-15 "communityget" Command

6.3.10 "dhget" Command

The command is to check the status and configuration of DHCP server.

Figure 6-16 "dhget" Command

6.3.11 "dhset" Command

The command is used to set DHCP function, such as server mode, Start IP, End IP, NTP server, DNS server and so on. Also, users are able to add, delete or update specified IP to specified MAC address via "Static Lease".

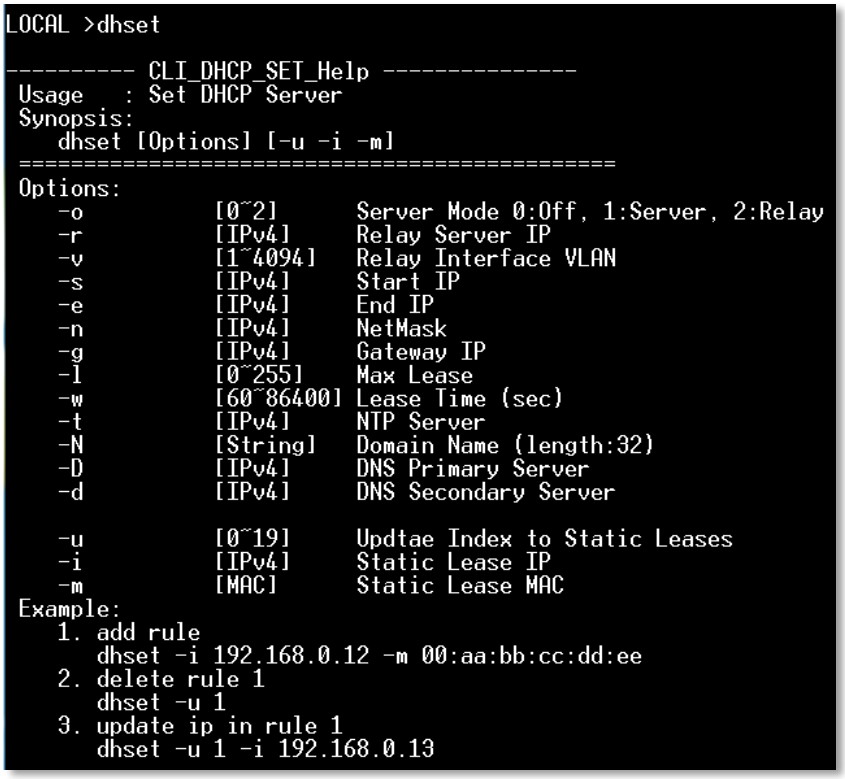


Figure 6-17 "dhset" Command

6.3.12 "dnsget" Command

The command is used to check DNS parameters, such as DNS settings, Cache settings and Authoritative Server settings.

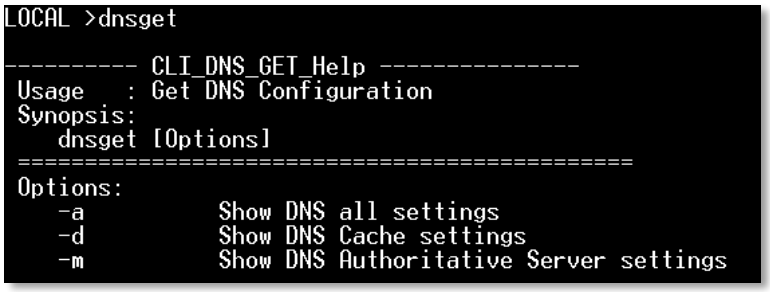


Figure 6-18 "dnsget" Command

6.3.13 "dnsset" Command

The command is used to set DNS configuration, TAINET prepares total examples for users as below command information.

```
LOCAL >dnsset

---------- CLI_DNS_SET_Help ---------------
 Usage   : Set DNS Configuration
 Synopsis:
    dnsset [Service Options]|[Zone Options]
 ============================================
 Service Options:
    -d          [0/1]       DNS Server Mode 0:OFF, 1:Cache
    -n          [String]    DNS Name
    -u          [0~2]       Upstream Server Index
    -i          [IPv4]      Upstream Server IP
    -t          [0~10]      Timeout (Sec)
    -m          [0/1]       Authoritative Server(AS) Mode 0:OFF, 1:ON
 Zone Options:
    -z          [1~3]       AS Zone Index
    -a          [0/1]       AS Zone Admin 0:OFF, 1:ON
    -s          [String]    AS Zone Domain Name
    -r          [1~8]       Update AS Zone Record Number
    -h          [String]    AS Zone Record Service Name
    -k          [IPv4]      AS Zone Record IP
    -l          [1~432000]      AS Zone Record Time To Live
 Example:
    1. Set DNS Cache Upstream Server 8.8.8.8, 8.8.4.4
       dnsset -u 1 -i 8.8.8.8 -u 2 -i 8.8.4.4
    2. Start DNS Cache with 6 seconds session timeout
       dnsset -d 1 -t 6
    3. Turn ON AS Zone 1 with Name "myexample1.net"
       dnsset -z 1 -a 1 -s myexample1.net
    4. Init Zone 2 and all record in it
       dnsset -z 2
    5. Add AS A+PTR Record at Zone 1
      ( mapping myexample1.net to 192.168.0.1 )
       dnsset -z 1 -k 192.168.0.1
    6. Update AS A+PTR Record at Zone 1 Record 2 (Zone:1.2)
      ( mapping www.myexample1.net to 192.168.0.2 as well )
       dnsset -z 1 -r 2 -h www -k 192.168.0.2
    7. Delete AS A+PTR Record at Zone 1 Record 3 (Zone:1.3)
       dnsset -z 1 -r 3
    8. Start Authoritative Server with name "mydns"
       dnsset -m 1 -n mydns
 Hint:
    Settings will work on after reset DNS Cache or AS.
```

Figure 6-19 "dnsset" Command

6.3.14 "exit" Command

Input "**exit**", and log out the system.

```
LOCAL >exit
CLI_EXIT



        Welcome to Tainet COMET


COMET login:
```

Figure 6-20 "exit" Command

6.3.15 "fmget" Command

The command is used to display and clear the current alarm logs.

```
LOCAL >fmget

 ---------- CLI_FMGET_Help --------------
 Usage   : Get FM
 Synopsis:
    fmget [Options]
 ============================================
 Options :
   -c    Clean alarm log
   -r    Get Real Time Alarm Log
   -a    Get Alarm Log

 Example :
   * Get alarm log
     fmget -a
```

Figure 6-21 "fmget" Command

6.3.16 "gset" Command

The command is used to set G.SHDSL parameters, such as CO/CPE mode, line rate, wire mode, line probe, EFM/ ATM/ HDLC mode and so on. Besides, Comet 160xFM only support EFM mode.

```
LOCAL >gset

 ---------- CLI_GSET_Help --------------
 Usage   : Set DSL parameter
 Synopsis:
    gset [options] [value]
 ============================================
 Options :
        -m  [ co/cpe setting ]  Control CO/CPE: '0':co mode, '1':cpe mode
        -r  [Line Rate]  Control  Line Speed (3~89)*64kbps
        -b  [PowerBackOff setting]  PBO: '0':disable, '1':enable
        -p  [PowerBackOff value Setting]      0~31 dB
        -w  [2/4/8 wire mode] wire mode: '0':2w , '1':4w , '2':8w ,'3':Auto
        -d  [syn/Aysn mode] psd mode: '0':sync mode, '1':async mode
        -x  [Annex-A/F Annex-B/G mode] '0':Annex-A/F mode, '1':Annex-B/G mode
        -y  [Line Probing] '1': disable, '2': enable
        -t  [SNR Target Margin] 0~21 dB
        -c  [Reference Clock] '1': mode 1, '2': 3a, '3':mode 2
        -o  [Mode] '0': EFM only, '1': Dual bearer, '2': Pure TDM '3': HDLC '4': ATM '5':hdlc+tdm
        -u  [Extended Mode] '0':disable, '1':enable (only in EFM mode is valid)
        -q  [Extended MaxRate ] (3~239)*64kbps
        -z  [Extended PAM] 1:4PAM, 2:8PAM, 3:16PAM, 4:32PAM, 5:64PAM, 6:128PAM
        -g  [Bonding Header] '0': disable, '1':enable
        -a  [AtnThreshold]           set  ( 0~ 127 )
        -s  [SNRMThreshold]          set  ( 0~ 15  )
        -v  [CRC-Threshold] set  ( 1~ 166 )  value
        -i  [Capability list]  '0': new, '1': old, '2':auto
        -f  [Topology Mode]  '0': point to point,
                             '1': p-to-mp (4w/8w<->n*2w),
                             '2' :mixed mode (8W<->2*4W),
                             '3': mixed mode (4w<->2*2w),
                             '4': p-to-mp (8W<->2*4W)
        -h  [DSL isolation]  '0': disable, '1': enable
        -j  [Auto sensing(EFM/ATM)]  '0': disable, '1': enable
Example:  Set DSL CO and Annex-B/G
          gset -m 0 -x 1
Example:  Set p-to-mp (4w/8w<->n*2w) mixed CO/CPE
          (loop1 is CPE)  gset  -n 0  -m 1
          (loop2 is CO)   gset  -n 1  -m 0
          (loop3 is CPE)  gset  -n 2  -m 1
          (loop4 is CO)   gset  -n 3  -m 0
```

Figure 6-22 "gset" Command

6.3.17 "get" Command

The command is used to check all G.SHDSL parameters.

```
LOCAL >get
-------------------- DSL configuration ----------------------
 DSL Mode                      CPE
  Wire                         Auto
  Linerate                     89
  Pbo                          Enable
  Pscale                       0 dB
  Psd                          Sync
  Annex                        Annex-B/G
  lineprobe                    Enable
  SNR Margin                   5 dB
  RefClock                     mode 3a
  mode                         EFMonly
  auto sensing(EFM/ATM)        Disable
  Extended Mode                Disable
  Extended PAM                 128_PAM
  Extended MaxRate             213
  Bonding Header               Enable
  AtnThres                     40 dB
  SnrThres                     5 dB
  Capability List              NEW
  topology mode                point to point
  isolation                    Disable
-------------------------------------------------------------
```

Figure 6-23 "get" Command

6.3.18 "rpget" Command

The command is used to check G.8032 parameters. Network managers can observe all online members in point to multi-point mode.

```
LOCAL >rpget

---------- CLI_G8032_GET_Help ---------------
 Usage   : Get G.8032 Information
 Synopsis: rpget [Option]
 ============================================

 Option  :
           -a   show g.8032 all information
           -c   show g.8032 configuration
           -s   show g.8032 status
```

Figure 6-24 "rpget" Command

6.3.19 "rpset" Command

The command is used to set G.8032 function. Firstly, go to "**-a**" to run the function. Whether it is DSL/ Ethernet ring topology or DSL serial linear network have some necessary parameters needed to be configured based on different scenarios.

```
LOCAL >rpset

---------- CLI_G8032_SET_Help ---------------
 Usage   : Set G.8032
 Synopsis: rpset {[Option]/[Member]}
 ============================================

 Option  :
   -a [0/1]     set admin 1:On , 0:Off
   -p [1~65535] set UDP port of group
   -n [1~65535] set ring number
   -v [1~4094]  set ring interface vlan
   -b [0/1]     set broadcast: 1:Global, 0:Local
   -o [0/1]     set character: 1:Owner, 0:Member
   -t [MAC]     set Owner MAC
   -l [1~5]     set link0: 1:Lan1, 2:Lan2, 3:Lan3, 4:Lan4, 5:DSL
   -k [1~5]     set link1: 1:Lan1, 2:Lan2, 3:Lan3, 4:Lan4, 5:DSL
   -r [0~6]     set RPL: 0:off, 1:Lan1, 2:Lan2, 3:Lan3, 4:Lan4, 5:DSL
   -e [0~255]   set packet repeat
   -D           send discovery packet
   -R [ALL/MAC] send request packet to all member or to specific one

 Member  :
   -u [0~250]   update member index 0~250
   -i [IPv4]    update member IPv4 address
   -m [MAC]     update member MAC address

 Example :
          1. Set group 0 as owner and enable G.8032.
             rpset -o 1 -a 1
          2. Insert member to G.8032 group 0
             rpset -i 192.168.0.1 -m aa:bb:cc:dd:ee:ff
          3. Update IP of member 10 in group 0
             rpset -u 10 -i 192.168.0.1
          4. Delete member 10 in group 0
             rpset -u 10
```

Figure 6-25 "rpset" Command

6.3.20 "ipset" Command

The command is to take effect in Bridge mode, the default parameter is port-based in VLAN rule equals to Bridge mode. Users can configure IP network by it.

```
LOCAL >ipset

---------- CLI_IPSET_Help ---------------
 Usage   : Set system ip address
 Synopsis:
    ipset [-i,-n,-g,-m] [ip]
 ============================================
 Options :
   -i    ip address
   -n    netmask address
   -g    gateway address
   -m    IP Mode 0:Static 1:DHCP
 Example :
   * Set IP, Network mask and default gateway.
     ipset -i 192.168.0.1 -n 255.255.0.0 -g 192.168.0.254
   * Unset default gateway
     ipset -g 0.0.0.0
   * Set IP with DHCP
     ipset -m 1
```

Figure 6-26 "ipset" Command

6.3.21 "ipv6get" Command

The command is used to check the device IPv6.

```
LOCAL >ipv6get
--------- IPV6 ----------
IPv6 Admin    : OFF
IPv6 IP       : ::192.168.0.1
IPv6 Prefix   : 64
IPv6 Route    :
-------------------------
```

Figure 6-27 "ipv6get" Command

6.3.22 "ipv6set" Command

The command is used to manually configure the IPv6, inclusive of IP, prefix and default gateway.

```
LOCAL >ipv6set

---------- CLI_IPV6_Help ---------------
 Usage   : User Interface Switch
 Synopsis:
     ipv6 [Option] [value]
 ============================================
 uisetset Options:
        -a              [0/1] 0:Off   1:On
        -p              [0~128] Prefix
        -i              [IPv6 Address] IP address
        -r              [IPv6 Address] default route
```

Figure 6-28 "ipv6set" Command

6.3.23 "lanset" Command

The command is used to set Ethernet parameters, such as admin status, LAN speed mode, ingress rate, egress rate and so on.

```
LOCAL >lanset

---------- CLI_LANSET_Help ---------------
Usage   : Set LAN parameter
Synopsis:
   lanset [Port] [Options]
=============================================
Port    [1~4] port identifier LAN1 ~ LAN4
Options :
  -a    [0/1] AdminStatus
        [0] Disable
        [1] Enable
  -s    [0~4] Lan Speed Mode
        [0] Auto Negotiation
        [1] 10-half
        [2] 10-full
        [3] 100-half
        [4] 100-full
  -f    [0/1] Flow Control
        [0] turn off
        [1] turn on
  -i    [0~10] ingress_rate setting
        [0] turn off
        [1] 64 kbps
        [2] 128 kbps
        [3] 256 kbps
        [4] 512 kbps
        [5] 1 Mbps
        [6] 2 Mbps
        [7] 5 Mbps
        [8] 10 Mbps
        [9] 20 Mbps
        [10] 50 Mbps
  -e    [0~10] egress_rate setting
        same as option -i
  -w    [0/1] Alarm Switch
        [0] Disable
        [1] Enable

Example :
  * Set LAN1 Admin on and Flow Control on
    lanset 1 -a 1 -f 1
  * Set LAN1 force speed 100 full
    lanset 1 -s 4
```

Figure 6-29 "lanset" Command

6.3.24 "langet" Command

The command is used to check all LAN parameters.

```
LOCAL >langet
------------------------------------------------------------------
                    |   LAN1
------------------------------------------------------------------
    AdminStatus     |   ON
    Speed           |   AUTO
    Flow_control    |   OFF
    Ingressrate     |   OFF
    Egressrate      |   OFF
    AlarmSwitch     |   OFF
------------------------------------------------------------------
                    |   LAN2
------------------------------------------------------------------
    AdminStatus     |   ON
    Speed           |   AUTO
    Flow_control    |   OFF
    Ingressrate     |   OFF
    Egressrate      |   OFF
    AlarmSwitch     |   OFF
------------------------------------------------------------------
                    |   LAN3
------------------------------------------------------------------
    AdminStatus     |   ON
    Speed           |   AUTO
    Flow_control    |   OFF
    Ingressrate     |   OFF
    Egressrate      |   OFF
    AlarmSwitch     |   OFF
------------------------------------------------------------------
                    |   LAN4
------------------------------------------------------------------
    AdminStatus     |   ON
    Speed           |   AUTO
    Flow_control    |   OFF
    Ingressrate     |   OFF
    Egressrate      |   OFF
    AlarmSwitch     |   OFF
```

Figure 6-30 "langet" Command

6.3.25 "load" Command

The command is used to load factory or default file, let users more convenient to establish the DSL connection.

```
LOCAL >load

Usage: Load profile       !
SYNOPSIS: load  [opt]
opt:
    -p      [1~ 2]        DSL Profile
    -u      [Name]        User Profile
    -d                    Software Default
    -D                    Hardware Default (Full Factory Default)
    -r                    Delete Profile
Example:
                load -p 2
                load -u Comet
                load -d
                load -r abc


---------------- User Profile List ----------------------
  1.                Comet |  2.      profile.default
---------------------------------------------------------
```

Figure 6-31 "load" Command

6.3.26 "maclg" Command

The command is used to get all ports' MAC learning table.

```
LOCAL >maclg

Usage: Get MAC Learning Table
SYNOPSIS: maclg a/c

options:
Example:  Get all port learning table

Example:  maclg a

Example:  Clear learning table

Example:  maclg c


LOCAL >maclg a
----------------------  show MAC Learning Table  ------------------
------------------------------------------------------------------------
Index:1   , Port1, VID:1   , MAC Address:00:0c:29:be:d1:6b
Index:2   , Port1, VID:1   , MAC Address:64:66:b3:74:90:48
Index:3   , Port1, VID:1   , MAC Address:9a:27:12:ec:14:0b
Index:4   , Port1, VID:1   , MAC Address:00:0c:29:53:04:a9
Index:5   , Port1, VID:1   , MAC Address:00:0b:fd:0d:0b:40
Index:6   , Port1, VID:1   , MAC Address:00:0c:2a:07:73:36
Index:7   , Port0, VID:1   , MAC Address:00:90:bb:f0:34:14
Index:8   , Port1, VID:1   , MAC Address:00:90:bb:18:06:6b
Index:9   , Port1, VID:1   , MAC Address:00:90:bb:f3:73:05
Index:10  , Port1, VID:1   , MAC Address:00:90:bb:f0:54:05
```

Figure 6-32 "maclg" Command

6.3.27 "natget" Command

The command is used to check NAT rules and each configuration.

```
LOCAL >natget

---------- CLI_NAT_GET_Help ---------------
 Usage   : Get NAT Information
 Synopsis:
    natget [Options]
 ============================================
 Options:
    -c          Show NAT Configuration
    -r          Show NAT Rules
    -t          Show ConnTrack Table
    -F          Flush and Show ConnTrack Table
```

Figure 6-33 "natget" Command

6.3.28 "natset" Command

The command is used to set NAT function. There are three main NAT items, "**SNAT**", "**MASQURADE**" and "**DNAT**". Different NAT definitions have different rules needed to be configured.

```
LOCAL >natset

---------- CLI_NAT_SET_Help ---------------
 Usage   : Set NAT Configuration/Rules
 Synopsis:
    dhset [Conf Opts] [Add Opts] [Delete Opts]
 ============================================
Conf Opts:
    -M    [0~8192]    Max ConnTrack
    -T    [0~432000]  Timeout of Established TCP (Sec)
    -U    [0~60]      UDP Timeout (Sec)
    -S    [0~600]     Timeout of UDP Stream (Sec)
Add Opts:
    -J    [1~3]       Nat Type 1:SNAT, 2:MASQUERADE, 3:DNAT
                      Opts only works with SNAT, MASQUERADE, DNAT
                      will be marked [a], [b], [c]
    -A    [1~3]       Add Rule To 1:PREROUTING 2:POSTROUTING 3:OUTPUT
    -i    [1~4094]    In-Face VLAN # , with Chain: PREROUTING only
    -o    [1~4094]    Out-Face VLAN # , with Chain: POSTROUTING, OUTPUT
    -N    [1~30]      Insert At Line Number #
    -P    [0,6,17]    Protocal 0:ALL 6:TCP, 17:UDP
                      Opts only works with ALL, TCP, UDP
                      will be marked [d], [e], [f]
    -s    [IPv4]      Source IP [a][b][c]
    -m    [0~32]      Source Mask [a][b][c]
    -p    [0~65535]   The Start of Source Port Range [e][f]
    -q    [0~65535]   The End of Source Port Range [e][f]
    -d    [IPv4]      Destination IP [a][b][c]
    -n    [0~32]      Destination Mask [a][b][c]
    -u    [0~65535]   The Start of Destination Port Range [e][f]
    -v    [0~65535]   The End of Destination Port Range [e][f]
    -t    [IPv4]      The Start of "To" IP Range [a][c]
    -e    [IPv4]      The End of "To" IP Range [a][c]
    -h    [1~65535]   The Start of "To" Port Range [e][f]
    -k    [1~65535]   The End of "To" Port Range [e][f]
Delete Opts:
    -D    [1~3]       Delete Rule In 1:PREROUTING 2:POSTROUTING 3:OUTPUT
    -N    [1~30]      Delete Rule Number #

Example:
    1. set configuration
       natset -M 4096 -T 432000 -U 30 -S 180
    2. Add SNAT rule 1
       natset -J 1 -A 2 -P 0 -s 172.15.5.199 -t 172.15.5.200 -o 1
    3. Del Rule 1 in Chain POSTROUTING
       natset -D 2 -N 1
```

Figure 6-34 "natset" Command

6.3.29 "pmset" Command

The command is used to clear all records of G.SHDSL performance.

```
LOCAL >pmset

---------- CLI_PMSET_Help ---------------
Usage   : Set PM parameter
Synopsis:
   pmset [TYPE] [Options]
================================================
TYPE :
  -g    DSL
  -e    E1
Options :
  -a    Clean all
  -m    clean_Current15min
  -d    clean_Current1Day
  -q    clean_History15min
  -s    clean_History1Day

Example :
  * Clear DSL all PM record
    pmset  -g -a
  * Clear E1 1Day History PM record
    pmset  -e -s
```

Figure 6-35 "pmset" Command

6.3.30 "pmget" Command

The command is used to check all records of G.SHDSL performance.

```
LOCAL >pmget

Usage: GET PM parameter
SYNOPSIS: pmget [Type] [Option] [Loop]
Type:
       -g: GSHDSL
Option:
       -f - Get pm_current_15
       -d - Get_pm_1_day
       -q - Get_pm_96_quarters
       -s - Get_pm_7_day
Loop:
       GSHDSL: Follow the loop count (1~4) of model
Example:
       pmget -g -f  1
```

Figure 6-36 "pmget" Command

6.3.31 "ping" Command

The command is used to verify the path of packet transmission between modem and other networks.

Figure 6-37 "ping" Command

6.3.32 "run" Command

The command is used to run all settings immediately.

Figure 6-38 "run" Command

6.3.33 "remote" Command (Comet 160xF only)

Connect local and remote modem to establish EOC-state, input "**remote**" to access the remote modem via EOC management, or input "local" back to the local configuration.

Figure 6-39 "remote" Command

6.3.34 "rmon" Command

The parameter is used to display G.SHDSL/Ethernet traffic statistics.

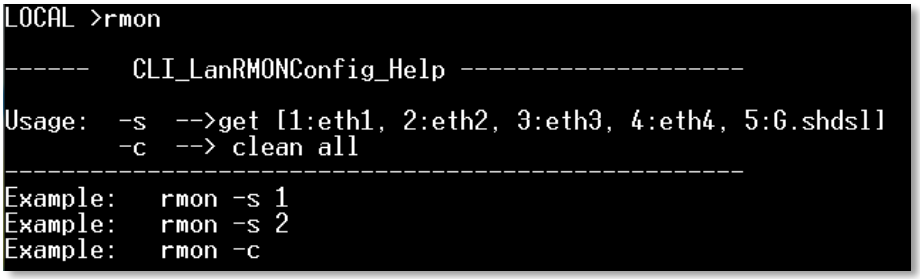


Figure 6-40 "rmon" Command

6.3.35 "sysset" Command

The command is used to set the system information, such as the system time, link security and reset.

```
LOCAL >sysset

 ---------- CLI_SYSSET_Help ---------------
 Usage   : Set system parameter
 Synopsis:
    sysset [Options]
 ============================================
 Options :
        -d      [YYYY-MM-DD-hh-mm-ss] DateTime
        -z      [1~85] TimeZone Number
   1: GMT-12:00   2: GMT-11:00   3: GMT-10:00   4: GMT-09:00   5: GMT-08:00
   7: GMT-07:00  10: GMT-06:00  14: GMT-05:00  17: GMT-04:30  18: GMT-04:00
  21: GMT-03:30  22: GMT-03:00  25: GMT-02:00  26: GMT-01:00  28: GMT+00:00
  30: GMT+01:00  35: GMT+02:00  42: GMT+03:00  46: GMT+03:30  47: GMT+04:00
  51: GMT+04:30  52: GMT+05:00  55: GMT+05:30  56: GMT+05:45  57: GMT+06:00
  62: GMT+06:30  63: GMT+07:00  65: GMT+08:00  71: GMT+09:00  74: GMT+09:30
  76: GMT+10:00  81: GMT+11:00  82: GMT+12:00  85: GMT+13:00
        -n      [IPv4] Ntp Server
        -e      [IPv4] Ntp Server 2
        -u      [0/1] NTP Auto-Update
        -c      [0~30] NTP Update Cycle (Day)
        -D      [0/1] Day Light Saving 0:Disabled  1:Enabled
        -l      [0/1] Link Security Switch  0:Disabled  1:Enabled
        -p      [000000~999999] Link Security Password
        -r      reset
        -s      0:Internal 1:E1 Interface 2:DP1 4:recovery from DSL
        -a      [0/1] Clock Auto Switching  0:Off , 1:On
        -w      [0/1] Interface(E1/Data Port) Alarm Switch  0:Off , 1:On
        -i      [String] System Description (length:32)
        -o      [String] System Contact (length:64)
        -m      [String] System Name (length:32)
        -j      [String] System Location (length:128)

 Example :
   * Set system time
     sysset -d 2016-08-18-12-34-561
   * Set Internal Clock to DSL
     sysset -s 0
```

Figure 6-41 "sysset" Command

6.3.36 "sysget" Command

The command is used to verify the system information. In general, users check IP network within Bridge mode, MAC address or software version at all.

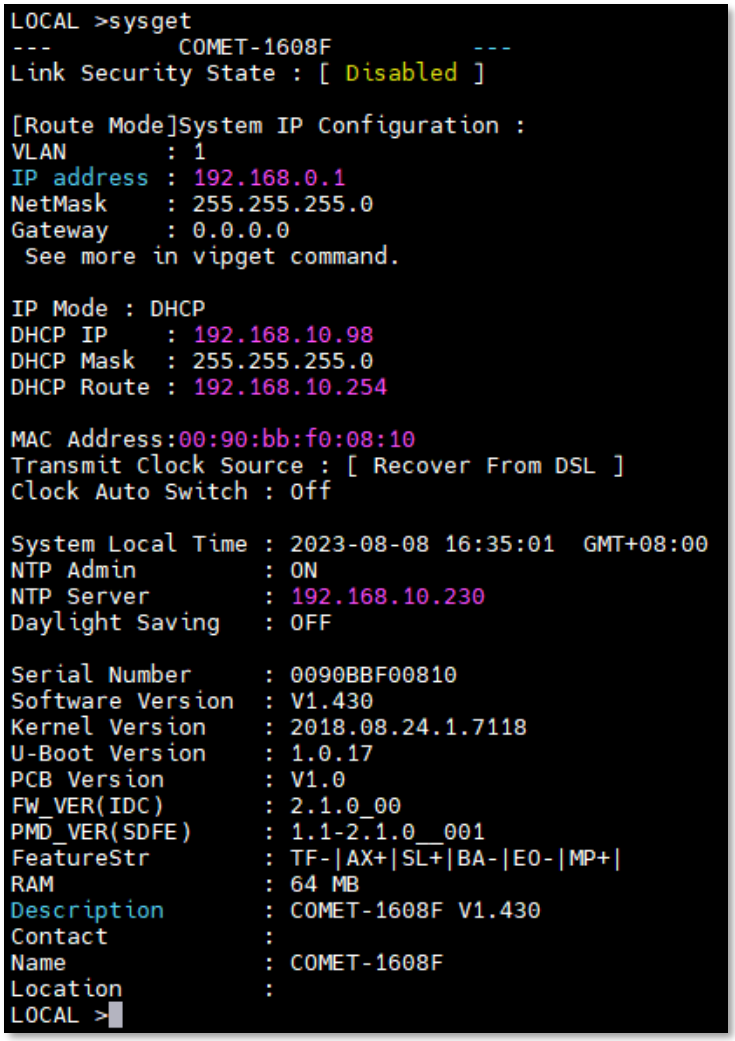


Figure 6-42 "sysget" Command

6.3.37 "show" Command

The command is used to show profile, startup or running configuration.

```
LOCAL >show

---------- CLI_SHOW_Help --------------
 Usage   : show configuration
 Synopsis:
    show [options]
 ============================================
 Options :
    -s           show startup-conf
    -r           show running-conf
    -p    [Name] Show User Profile Config
    -f           show profile list

---------------- User Profile List --------------------
  1.               Comet |  2.      profile.default
-------------------------------------------------------

 Example :
   * show running-config
     show -r
```

Figure 6-43 "show" Command

6.3.38 "status" Command

The command is used to check G.SHDSL status. Most of all, network managers check the DSL connection and current line rate.

```
LOCAL >status

-----------------------------------------
--- Show DSL / LAN PORT status
--- DSL1 --------------------------
 Linkstate    Connected
 EOC-state        Ready
 Linerate     5696
 Annex        Annex-B
 TC_PAM       TC_PAM32
 Pscale       5 dB
 Atn          0 dB
 Snr          18 dB
 ---Loopback State ---
               Normal
-----------------------------------------------------------------
---------  LAN1 ---------------------------------------------------
 LinkStatus          Link up
 Speed               100 Full
-----------------------------------------------------------------
-----------------------------------------------------------------
---------  LAN2 ---------------------------------------------------
 LinkStatus          Link down
 Speed               10 Half
-----------------------------------------------------------------
```

Figure 6-44 "status" Command

6.3.39 "snmpv3get" Command

The command is used to check SNMPv3 function, such as username, rights and security protocol.

```
LOCAL >snmpv3get

User Name : admin
Security Level : auth & priv
Auth Algorithm : SHA
Auth Password : ********
Privacy Algorithm : AES
Privacy Password : ********
```

Figure 6-45 "snmpv3get" Command

6.3.40 "snmpv3set" Command

The command is used to set SNMPv3 function. Different security levels, passwords and algorithms needed to be configured.

```
LOCAL >snmpv3set

Usage: Setup SNMP V3 Configuration!
SYNOPSIS: snmpv3set [option] [value]
options:
        -u  Add USM User Name:[max--16]
        -s  Security Level [0:no auth & no priv, 1:auth & no priv, 2:auth & priv]
        -a  Auth Algorithm [0:MD5, 1:SHA]
        -p  Auth Password: [max--16, least--8]
        -r  Privacy Algorithm [0:DES, 1:AES]
        -w  Privacy Password: [max--16, least--8]]
        -d  Delete USM User
Example: snmpv3set -u xxxx -s 2 -a 0 -p xxxxxxxx -r 0 -w xxxxxxxx
Example: snmpv3set -u xxxx -s 1 -a 0 -p xxxxxxxx
Example: snmpv3set -u xxxx -s 0
Example: snmpv3set -d xxxx
```

Figure 6-46 "snmpv3set" Command

6.3.41 "save" Command

The command is used to save all settings after configured.

```
LOCAL >save
Save Success.
```

Figure 6-47 "save" Command

6.3.42 "tacget" Command

The command is used to get TACACS+ information.

```
LOCAL >tacget
-------------------------- TACACS+ --------------------------
 Admin               : OFF
 Server              : 0.0.0.0
 Port                : 49
 Secret              : ******
 Authentication      : CHAP
 Service Type        : raccess
 Priority Attr.      : priv-lvl
-------------------------------------------------------------
```

Figure 6-48 "tacget" Command

6.3.43 "tacset" Command

The command is used to set TACACS+ function.

```
LOCAL >tacset

---------- CLI_TACACS_SET_Help ---------------
 Usage   : Set TACACS+
 Synopsis:
    tacset [options]
 ============================================
 Options :
    -a    [0/1]       Admin (1)ON (0)OFF
    -s    [IPv4]      Server
    -p    [0~65535]   Port
    -c    [str]       Secret
    -t    [0~2]       Auth Type
                      0:ASCII
                      1:PAP
                      2:CHAP
    -S    [String]    Service of AV Pair to Server
    -P    [String]    Priority Attribute of AV Pair from Server
 Example :
   * Set TACACS
     tacset -a 1 -s 172.16.2.107 -p 49 -c test -t 2
   * Unset TACACS secret
     tacset -c ''
   * Set Author AV Pair : 'service=raccess' and expect 'priv-lvl
     tacset -S raccess -P priv-lvl
```

Figure 6-49 "tacset" Command

6.3.44 "rstpg" Command

The command is used to get RSTP Parameter and Status.

```
LOCAL >rstpg
|Port Index   | Status         | Role           | Path Cost | Type           |
|-------------|----------------|----------------|-----------|----------------|
|LAN1         | Forwarding     | NonStp         | 19        | edge           |
|LAN2         | Forwarding     | NonStp         | 19        | edge           |
|LAN3         | Forwarding     | NonStp         | 19        | edge           |
|LAN4         | Forwarding     | NonStp         | 19        | edge           |
|DSL          | Forwarding     | NonStp         | 62        | edge           |
|-------------|----------------|----------------|-----------|----------------|

RSTP Status
STP Designated Root            :  8000.0090bbf00815
STP Bridge ID                  :  8000.0090bbf00815
STP Root Path Cost             :  0
STP Forward delay (sec)        :  15
STP Hello time (sec)           :  2
STP Max Age (sec)              :  20

RSTP Configuration
RSTP Mode                      :  Off
Bridge Priority                :  32768
Bridge Forward Delay (sec)     :  15
Bridge Hello Time (sec)        :  2
Bridge Max Message Age (sec)   :  20
```

Figure 6-50 "rstpg" Command

6.3.45 "rstps" Command

The command is used to set RSTP parameter, such as the RSTP mode and Bridge priority.

```
LOCAL >rstps

---------- CLI_STPSET_Help ---------------
 Usage   : Set RSTP Parameter
 Synopsis:
    rstps [options] [value]
 ============================================
 Options :
    -m      RSTP mode (0:Off, 1:On)
    -p      Bridge priority (0~61440) in steps of 4096
    -f      Bridge forward delay (4~30(s))
    -a      Bridge max message age (6~40(s))
    -h      Bridge hello time (1~10(s))
 Example :
    RSTP mode enable, bridge priority:32
    rstps -m 1 -p 32
```

Figure 6-51 "rstps" Command

6.3.46 "tftp" Command

The command is used to upgrade the modem via TFTP server. Users have to prepare a workable TFTP server first and put the firmware in the download path. In the end, back to the modem configuration for setting the correct IP, file path and file name.

```
LOCAL >tftp

---------- CLI_TFTP_Download_Help --------------
 Usage   : Upgrade
 Synopsis:
   tftp [Option] value


 ============================================
 tftp Options:
     -i   [ipv4]   IP
     -d   [file]   (1) Download image and upgrade firmware
                   (2) Download profile
                   must include extended name
     -u   [file]   Upload profile

---------------- User Profile List --------------------
  1.               Comet |  2.      profile.default
-------------------------------------------------------

 tftp Options:
    * Download image and upgrade firmware
      tftp -i 172.16.2.114 -d COMET165x_Download_V1.340.img
    * Download profile
      tftp -i 172.16.2.114 -d aaa.profile
      tftp -i 172.16.2.114 -d folder/bbb.profile
    * Upload profile
      tftp -i 172.16.2.114 -u ccc.profile
```

Figure 6-52 "tftp" Command

6.3.47 "tr069s" Command

The command is used to set TR-069 function. Modems act as TR-069 clients. In the protocol, clients have its own authentication, and need to follow to server's definition. Remember to check both sides are having the same parameters.

```
LOCAL >tr069s

Usage: Set TR069 Configuration !
SYNOPSIS: tr069s [options] [value]
options:
        -m  [TR069 mode]  '0':disable, '1':enable
        -u  [ACS URL]  (max:255 char)
        -a  [Login ACS user name]  (max:255 char)
        -b  [Login ACS password]  (max:255 char)
        -p  [CPE Port] [1000~65535]
        -c  [Connection request user name] [max:255 char]
        -d  [Connection request password] [max:255 char]
        -t  [CPE auth] '0':disable, '1':enable
        -e  [Periodic inform] '0':disable, '1':enable
        -i  [Periodic interval] [1~86400(s)]
        -v  [SOAP ENV] (max:31 char)
        -s  [SOAP ENC] (max:31 char)
Example: tr069s -m 1 -u http://192.168.0.21:8080/ -p 5400
                -v SOAP-ENV -s SOAP-ENC
```

Figure 6-53 "tr069s" Command

6.3.48 "tr069g" Command

The command is used to check TR-069 parameters, such as mode, CPE port ACS URL and so on.

```
LOCAL >tr069g

TR069 mode: Disable
CPE port: 5400
CPE authentication: Enable
Connection request user name: cwmp
Connection request password: ****
ACS URL: http://192.168.1.21:8080/
Login ACS user name: acsacs
Login ACS password: ****
Periodic inform: Disable
Periodic interval: 300(sec.)
SOAP ENV: SOAP-ENV
SOAP ENC: SOAP-ENC
```

Figure 6-54 "tr069g" Command

6.3.49 "trapset" Command

The command is used to set SNMP trap IP, trap status, duplication and repeat interval.

```
LOCAL >trapset

Usage:
  Set Trap Configuration
Synopsis:
  trapset [Target Options][General Options]

Target Options:
   -i  [1~5] trap index
   -s  [IPv4] trap server ip
   -t  [1~3] trap type [0:OFF, 1:SNMP, 2:Syslog, 3:SNMP+Syslog]

General Options:
   -d  [0|1] trap duplication, 0:close, 1:open
   -r  [0-1440] repeat interval (minutes) , 0:close, others:i mins
   -v  [2~3] snmp trap version
   -u  [1~10] snmp trap user
       [  1] User Name          : admin
             Security Level     : auth & priv

Example:
   * set trap entry index 1 server 172.16.0.104 with SNMP+syslog
     trapset -i 1 -s 172.16.0.104 -t 3
   * set SNMP trap version 3 and use user 1 to auth and encrypt
     trapset -v 3 -u 1
   * set trap duplication with interval 5 minutes
     trapset -d 1 -r 5
```

Figure 6-55 "trapset" Command

6.3.50 "trapget" Command

The command is used to display trap IPs.

```
LOCAL >trapget

------------ Trap Server List ----------------------------
 Index |  SNMP  | Syslog | Trap Server IP
-------------------------------------------------------
     1 |        |        | 0.0.0.0
-------------------------------------------------------
     2 |        |        | 0.0.0.0
-------------------------------------------------------
     3 |        |        | 0.0.0.0
-------------------------------------------------------
     4 |        |        | 0.0.0.0
-------------------------------------------------------
     5 |        |        | 0.0.0.0
-------------------------------------------------------

------------ Trap SNMP Configuration ---------------------
 SNMP Trap Version  : 2C
 SNMP Trap User     : [0] None
-------------------------------------------------------
------------ Trap Duplication ----------------------------
 Trap Duplication   : ON
 Repeat Interval    : 5 mins
-------------------------------------------------------
```

Figure 6-56 "trapget" Command

6.3.51 "userset" Command

Comet 160xF/ FM and 160xF-R/ FM-R support three levels of security authority, inclusive of "**Administrator**", "**Operator**" and "**Monitor**". In the mechanism, the highest authority of operator is able to manage all functions, such as add, delete or modify, just remember to follow the password rules.

```
LOCAL >userset

Usage: Set system user information !
SYNOPSIS: userset [-a] [name] [admin_password] [password] [rights]
          userset [-d] [name] [admin_password]
          userset [-p] [name] [admin_password] [password]
          userset [-r] [name] [admin_password] [rights]
Options: [-a] - add user
         [-d] - delete user
         [-p] - modify user password
         [-r] - modify user rights
rights: 1 -- Admin
        2 -- Operator
        3 -- Monitor
Password Rule: comply with 2 rules below
               1. include a numbers 0~9
               2. include a upper case letter A~Z
               3. include a upper case letter a~z
               4. include a sign (exclude space)
```

Figure 6-57 "userset" Command

6.3.52 "userget" Command

The command is used to check all users' accounts and rights except of passwords.

```
LOCAL >userget
User Name : admin
User Password : *****
User Rights : Admin
------------------------------
User Name : guest
User Password : *****
User Rights : Monitor
------------------------------
User Name : user
User Password : ****
User Rights : Operator
------------------------------
```

Figure 6-58 "userget" Command

6.3.53 "uiget" Command

The command is used to check all user interfaces.

```
LOCAL >uiget

---------- User Interface ----------
Telnet          : Permit      23
SSH             : Permit      22
HTTP            : Permit      80
HTTPS           : Permit     443
SNMP            : Permit     161
Protection      : ON
Idle Timeout    : 5 minutes
-----------------------------------


---------- Management List ---------
 Index | Management IP/Mask
-----------------------------------
     1 | 0.0.0.0/24
-----------------------------------
     2 | 0.0.0.0/24
-----------------------------------
     3 | 0.0.0.0/24
-----------------------------------

------------ List of Refused IP ------------------------------------------------
 Index |      IP                                          | Reconnect Time
              Null
--------------------------------------------------------------------------------
```

Figure 6-59 "uiget" Command

6.3.54 "uiset" Command

The command is used to set user interface, such as Telnet, SSH, HTTP, HTTPS and account protection.

```
LOCAL >uiset

---------- CLI_UISET_Help ---------------
 Usage   : Set User Interface Configuration
 Synopsis:
     uiset [General Options] [Access Options]
 ============================================
 General Options:
    -t    [0/1]     0:Telnet Limited  1:Permit Telnet
    -T    [1~65535] Telnet Port
    -s    [0/1]     0:SSH Limited  1:Permit SSH
    -S    [1~65535] SSH Port
    -h    [0/1]     0:HTTP Limited  1:Permit HTTP
    -H    [1~65535] HTTP Port
    -p    [0/1]     0:HTTPS Limited  1:Permit HTTPS
    -P    [1~65535] HTTPS Port
    -n    [0/1]     0:SNMP Limited  1:Permit SNMP
    -N    [1~65535] SNMP Port
    -a    [0/1]     0:Close A.P.    1:Open Account Protection
    -c    [1]       Clear All Refused IP
    -o    [5~1440]  Idle Timeout (minutes)

 Access Options:
    -u    [1~3]     Index
    -i    [IPv4]    Management IP

 Example:
    * set Management IP/Mask entry 1 as 10.10.1.1/16
      uiset -u 1 -i 10.10.1.1/16
    * set telnet can only accessed by Management IP/Mask
      uiset -t 0
    * Flush All Refused IP
      uiset -c 1
```

Figure 6-60 "uiset" Command

6.3.55 "vipget" Command

The command is used to check "**Virtual IP**" in routing mode.

```
LOCAL >vipget

---------- CLI_VIP_GET_Help ---------------
 Usage   : Get Virtual IP Settings
 Synopsis:
    vipget [Options]
 ============================================
 Options:
    -a          Show ALL Settings on VIPs
    -i          Show IP table only
```

Figure 6-61 "vipget" Command

6.3.56 "vipset" Command

The command is used to set "**Virtual IP**" in routing mode. Users have to follow the rules to create, delete or update Virtual IPs.

```
LOCAL >vipset
Incomplete format.

---------- CLI_VIPSET_Help ---------------
 Usage   : Set Virtual IP
 Synopsis:
    vipset [Options]
 ============================================
 Options:
    -m          [0~3]    IP Mode 0:Static IP, 1:DHCP, 2:PPPoE, 3:PPTP
    -v          [1~4094] VLAN Interface
    -d          [1~30]   Delete/Update rule x
    -i          [IPv4]   IP
    -n          [IPv4]   Netmask
    -g          [IPv4]   Gateway
    -t          [IPv4]   Secondary IP
    -y          [IPv4]   Secondary Netmask
    -w          [string] PPPoE/VPN Desired Service-Name
    -a          [string] PPPoE/VPN Name
    -p          [string] PPPoE/VPN Password
    -s          [IPv4]   VPN Server
    -G          [0/1]    Default Gateway 1:ON(default), 0:OFF
    -S          [0/1]    DHCP Server Service 1:ON(default), 0:OFF
    -N          [0/1]    DNS Service 1:ON(default), 0:OFF
    -R          [0/1]    Router Service 1:ON(default), 0:OFF
 Example:
    1. add static IP rule on vlan 100
       vipset -v 100 -i 10.1.0.1 -n 255.255.0.0 -g 10.1.0.254
    2. delete rule
       vipset -d 1
    3. update rule ip, vlan
       vipset -d 1 -i 10.2.0.2 -v 200
    4. update vlan 1 : VPN Password and unset Desired Service-Name
       vipset -d 1 -p admin -w ''
```

Figure 6-62 "vipset" Command

6.3.57 "vrget" Command

The command is used to check routing rules in routing table. Routing rules include "**Full Routing Table**", "**Dynamic Routing Settings**", "**Static Routing Rules**" and "**Dynamic Routing Service Interface**".

```
LOCAL >vrget

---------- CLI_VR_GET_Help ---------------
 Usage   : Get Routing Information
 Synopsis:
    vrget [Options]
 ============================================
 Options:
    -a          Show All
    -f          Show Full Routing Table
    -d          Show Dynamic Routing Settings
    -s          Show Static Routing Rules
    -i          Show Dynamic Routing Service Interface
```

Figure 6-63 "vrget" Command

6.3.58 "vrset" Command

The command is used to set routing rules. One of main function is named "Static Route", in order to manually add or delete rules. Also, RIPv1 & RIPv2 are configurable.

```
LOCAL >vrset

---------- CLI_VRSET_Help -------------------
 Usage   : Set Routing Rules
 Synopsis:
    vrset [Options]
 ============================================
 Options:
     -v      [1~4094] VLAN Tag
   Dynamic :
     -m      [0~4]   Dynamic Routing Mod
             [0] OFF
             [1] RIPv1
             [2] RIPv2
             [3] OSPFv2
             [4] BGP-4
     -h      [10~60] OSPF Hello Interval (Sec)
     -t      [40~240] OSPF Dead Timeout Interval (Sec)
     -p      [0~255] OSPF Priority
     -a      [u32/ipv4] OSPF Area
     -c      [u32]   OSPF Metric Cost
     -b      [1~65535] BGP Local ASN
     -e      [0/1]   BGP ebgp-multihop
     -r      [ipv4]  BGP Peer
     -s      [1~65535] BGP Peer ASN
     -w      [u32]   BGP Neighbor Weight
     -f      [u32]   BGP Neighbor Local Preference
     -o      [u32]   BGP Neighbor Metric Cost
     -x      [ipv4]  BGP Neighbor Next Hop
     -y      [ASN:u16/u32] BGP Neighbor Community
             internet      =     0:0
             no-export     = 65535:65281
             no-advertise  = 65535:65282
             local-AS      = 65535:65283
   Static :
     -d      [1~30]   Delete rule x
     -i      [IPv4]   Destination domain
     -n      [IPv4]   Netmask
     -g      [IPv4]   Gateway
```

Figure 6-64 "vrset" Command

6.3.59 "vrrpget" Command

The command is used to get VRRP Information.

```
LOCAL >vrrpget
------------- VRRP Configuration ---------------------------------------------
 Interface | Entry | Admin | State    | ID  | Pri / Track | IP
-------------------------------------------------------------------------------
 eth0.1    | 1     | OFF   | --       |   1 | 100 / LAN1  | 0.0.0.0
           | 2     | OFF   | --       |   1 | 100 / LAN1  | 0.0.0.0
-------------------------------------------------------------------------------
```

Figure 6-65 "vrrpget" Command

6.3.60 "vrrpset" Command

The command is used to set VRRP parameter, such as Interface VLAN, Priority, and VRRP IP.

```
LOCAL >vrrpset

---------- CLI_VRRP_SET_Help ---------------
 Usage   : Set VRRP
 Synopsis:
    vrrpset [options]
 ============================================
 Options :
    -v    [0~4094] Interface VLAN
    -e    [1~2]    Entry
    -a    [0/1]    Admin (1)ON (0)OFF
    -r    [0~255]  Router ID
    -p    [0~255]  Priority
    -i    [IPv4]   VRRP IP
    -t    [1~5]    Port Tracking per interface (priority -20 while port down)
          [1~4]    LAN1 ~ LAN4
          [5]      DSL
 Example :
   * Set VRRP entry up with specific ip, id and priority
     vrrps -v 1 -e 1 -a 1 -r 10 -p 100 -i 10.1.2.3
   * Set VRRP vlan 1 port tracking on LAN1
     vrrps -v 1 -t 1
```

Figure 6-66 "vrrpset" Command

Appendix A Pin Assignment

A.1 Console Pin Assignment

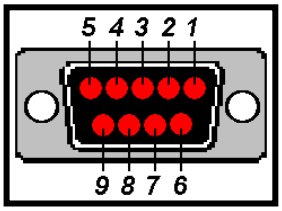


Figure A-1 DB-9 Interface

DB-9 Pin	Description
1	NC
2	TxD (Out)
3	RxD (In)
4	NC
5	GND
6~9	NC

Console RJ-45 to DB-9 pin assignment is as the following:

RJ-45 Pin	Description	DB-9 Pin
1~2	NC	
3	RXD	DB-9 pin2 (Output)
4	GND	DB-9 pin5
5	TXD	DB-9 pin3 (Input)
6~8	NC	

Table A-1 RJ-45 to DB-9 pin assignment

A.2 DSL RJ-45 Pin Assignment

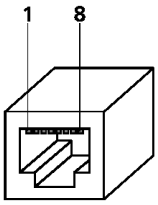


Figure A-2 DSL RJ-45 Pin Assignment

Pin	8W	4W	2W
1	Tip(2)		
2	Ring(2)		
3	**Tip(4)**	Tip(2)	
4	Tip(1)	Tip(1)	Tip
5	Ring(1)	Ring(1)	Ring
6	**Ring(4)**	Ring(2)	
7	Tip(3)		
8	Ring(3)		

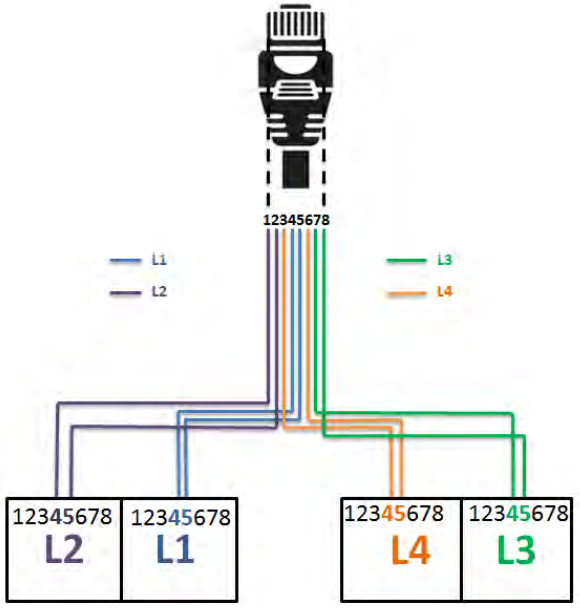
A.3 DSL RJ-45 Pin Assignment (Comet 160xFM)

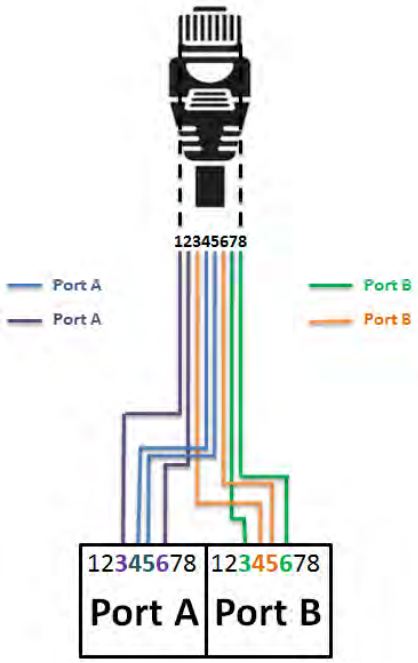
The Port A is as default software configured CPE mode and Port B is CO. On the contrary, once if software configured device to **CO** then Port A will be CO and Port B side is CPE.

Current Device Mode	Port A	Port B
CPE (Default)	CPE	CO
CO	CO	CPE

Pin	2W	4W	8W	PortA	PortB
1			Tip(2)		
2			Ring(2)		
3		Tip(2)	Tip(4)	Tip(2)	Tip(3)
4	Tip(1)	Tip(1)	Tip(1)	Tip(1)	Tip(4)
5	Ring(1)	Ring(1)	Ring(1)	Ring(1)	Ring(4)
6		Ring(2)	Ring(4)	Ring(2)	Ring(3)
7			Tip(3)		
8			Ring(3)		

DSL 1 to 4	DSL 1 to 2
4Wire / 8Wire <-> N x 2Wire	8Wire <-> 2 x 4Wire
8Wire <-> 2 x 4Wire	4Wire <-> 2 x 2Wire





A.4 LAN RJ-45 Pin Assignment

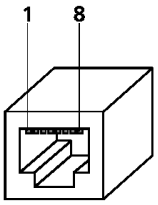


Figure A-3 LAN RJ-45 Pin Assignment

Pin	Description
1	RxD+
2	RxD -
3	TxD-
4	NC
5	NC
6	TxD+
7	NC
8	NC

A.5 Comet 160xF/ FM, 160xF-R/ FM-R DIP switches

Figure A-4 16xxF/160xFM DIP switches

DIP	1	2
ON	Factory Profile CO Mode	Ser2Net
OFF	User Profile / CPE Mode	Reserved

As both of DIP switches are setup to "OFF", and then power on. The Comet 160xF will load the latest user's profile which it has been saved before in system. In default settings, it acts as **CPE** mode with IP address 192.168.0.1. When operators would like to do any changes on modem and save it, the modem will load the new boot profile in next power on.

If only **DIP1** switch is setup to "ON", and then power on. The Comet 160xF will load the **CO**'s factory profile and run the IP address it was used before. If operator did some changes on configuration and saved to user's profile, the system will do the new configuration, as well.

** The IP address will change whenever operator clicks "APPLY" and kept in system NVRAM by "save" command. The NVRAM for IP address is different from user's profile, so the user's profile will not save the IP address but only for related configurations. **

Appendix B Trouble Report

Company	
Local Representation	
Purchase Order No	
Equipment Serial No	
Software Version	

Please describe: 1. Testing Network Structure 2. Configuration
3. Testing Network Equipment 4. Trouble Description

E-MAIL:	
TEL:	FAX:
Signature:	Date: / /

TAINET COMMUNICATION SYSTEM CORP.
FAX: 886-2-2793-8000
E-MAIL: **sales@TAINET.net**