User Manual

ML630R

G.SHDSL L3 CPE

User Manual

Release R1.0

Revision No. A05

Actelis Networks®

Document No. 520R69691E

Preface Material

Document Identification

ML630R

Document No. 520R69691E

Revision No. A05

Date: Aug 2021

Copyright

Disclaimer of Warranties and limitation of Liabilities

Actelis Networks, Inc. (hereafter referred to as Actelis Networks, Inc. or Actelis Networks), makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, in no event, shall Actelis Networks be liable for incidental or consequential damages in connection with or arising from the use of the ML630R series, modules, accessories kits, this manual or any related materials. Actelis Networks reserves the right to revise this publication from time to time and to make changes in the content hereof without obligation to notify any person of such revisions or changes.

Trademarks

Actelis, Actelis Networks, EFM*plus*, MetaASSIST, Carrier Ethernet over Copper and related logos and icons are the registered trademarks or copyrights of Actelis Networks. Other identifiers may be trademarks or marks of their respective owners.

Document Objectives

This manual provides a general description of the ML630R device, detailed instructions for the deployment and maintenance of the ML630R.

Intended Audience

The intended audience for this document is both technical and non-technical staff within Network Service Provider (NSP) organizations, and it is assumed that the reader has a general understanding of voice and data communications, the xDSL industry and high-speed digital services.

Contact Information

Please contact your local sales representative, service representative or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training or distributor locations, use any one of the following:

- **Internet:** Visit the **Actelis Networks World Wide Web site http://www.Actelis.com**
- **Mail to: Actelis Networks customer support Mailto: techsupport@actelis.com** for technical support.
- **Customer support:** Contact Actelis Networks Customer Support directly at one of the following numbers:
  - Belgium: (0) 800 71180
  - Denmark: 80 887 771
  - France: (0) 800 918 450
  - Germany: (0) 800 1833504
  - Netherlands: (0) 800 0225982
  - UK: (0) 800 9179049
  - USA: +1 866 638 2544 or +1 510 545 1071

  For all other inquiries, please call +1 866 ACTELIS (+1 866 228 3547) or +1 510 545 1071.

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Actelis Networks, 47800 Westinghouse Drive, Fremont, CA 94539 or to **userdoc@actelis.com mailto:userdoc@actelis.com**. Include the document number, revision number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

ML630R Certification

FCC Class A Compliance

ML630R models, which comply with the limits for class A) comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules.

Warning: ML630R models are Class A product. In a domestic environment, this product may cause radio interference, in which case you may be required to take adequate measures.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with this document may cause harmful interference to radio communications.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Actelis Networks, Inc.

CE Mark

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.

Safety:

EN 60950-1, IEC 60950-1

EMC:

CISPR 32, EN 55032, EN 55024, EN 61000-3-2, EN 61000-3-3

ISO 9001 Quality Management

China CCC Quality Certification

Directives: LVD 2006/95/EC, EMC 204/108/EC, and RoHS 2011/65/EU.

CE

This product complies with the requirements of the Low Voltage Directive 73/23/E and EMC Directive 89/336/EEC as amended by 92/31/EEC and 93/68/EEC, when it is properly installed and maintained, and when it is used for the purposes for which it is intended.

General Safety Instructions

1. Read and follow all warning notices and instructions marked on this product or included in this manual.
2. All installation, repair or replacement procedures must be performed by qualified service personnel.
3. Before attempting to operate or repair this product, make sure product is properly grounded.
4. This product uses an external power source. Do not touch exposed connections, components or wiring when power is present.
5. Do **not** operate this product with panels removed or with suspected failure or damage to electrical components.
6. Do **not** operate or repair this product in wet or damp conditions or in an explosive atmosphere.
7. Keep product surfaces clean and dry.
8. Provide proper ventilation.
9. Observe all ratings and markings on the product. Before making connections to the product, consult the appropriate chapters of this manual for further ratings information.
10. Cables that are supplied by the customer must comply with the regulatory inspection authorities and are the responsibility of the customer. To reduce the risk of fire, make sure all cables are UL Listed or CSA Certified.
11. This equipment must be installed according to country national electrical codes. For North America, equipment must be installed in accordance with the US National Electrical Code, Articles 110–16, 110–17 and 110–18 and the Canadian Electrical Code, Section 12. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
12. Over-current Protection: It is recommended to incorporate in the building wiring, a readily accessible listed branch circuit overcurrent protective device rated to 2A min. and 5A max. A 5A circuit over current protective device can feed two ML630R units in rack mount shelf.
13. The equipment shall be connected to a properly earthed supply system.
14. All equipment in the immediate vicinity shall be earthed the same way and shall not be earthed elsewhere
15. A disconnect device is not allowed in the earthed circuit between the DC supply source and the frame/earthed circuit connection.

Prevention of Electrostatic Discharge (ESD) Damage

1. When working with electronic components, wear a commonly grounded antistatic wrist strap to discharge the static voltage from your body in accordance with approved standards.
2. Do not use any devices capable of generating or holding a static charge in the work area where you install or remove electronic components. Avoid handling electronic components in areas that have a floor or benchtop surface capable of generating a static charge.
3. Do not slide electronic components over any surface. Do not touch exposed connector pins. Handle electronic components as little as possible.
4. Transport and store electronic components in an approved static-protected bag or container.

Consumer Notice

The purchased Actelis' product is subject to Directive 2002/96/EC of the European Parliament and the Council of the European Union on waste electrical and electronic equipment (WEEE) and, in jurisdictions adopting that Directive, is marked as being put on the market after August 13, 2005, and should not be disposed of as unsorted municipal waste. Please utilize your local WEEE collection facilities in the disposition of this product and otherwise observe all applicable requirements.

Résumé des conditions générales de sécurité

1. Lisez et suivez attentivement les notes d'avertissements et les instructions indiquées sur ce produit ou inclues dans ce manuel.
2. Toute installation, procédure d'entretien ou de remplacement doit être effectuée par un personnel de service qualifié.
3. Avant d'essayer de faire fonctionner ou de réparer ce produit, veillez à ce que le produit soit connexion de mis à la terre correctement.
4. Ce produit utilise une source de courant externe. Veuillez ne pas toucher les connections, éléments ou fils électriques découverts quand il y a du courant.
5. **Ne** faites pas fonctionner ce produit sans ses panneaux ou si vous suspectez une défaillance ou un dégât au niveau des composants électriques.
6. **Ne** faites pas fonctionner ce produit dans des conditions mouillées ou humides ou dans une situation où il y a risque d'explosion.
7. Gardez les surfaces du produit propres et sèches.
8. Fournissez une aération appropriée.
9. Observez toutes les valeurs nominales et indications sur le produit. Avant d'établir des connexions au produit, consultez les chapitres du manuel pour obtenir plus d'informations sur les évaluations.
10. De nombreux câbles de ce produit sont fournis par la société Actelis Networks. Les câbles qui sont fournis par le client doivent adhérer aux normes des autorités d'inspection et relèvent de la responsabilité du client. Pour diminuer le risque d'incendie, assurez vous que les câbles soient sur la liste UL ou certifiés CSA.
11. Cet équipement doit être installé en fonction des codes d'électricité du pays. En Amérique du Nord, l'équipement doit être installé suivant le Code National d'Electricité Américain, Articles 110-16, 110-17 et 110-18 et suivant le Code d'Electricité Canadien, Section 12. Si nécessaire, consultez les organismes de réglementation et les autorités d'inspection appropriés pour vous assurer de la conformité de l'installation.
12. Protection en cas de courant excessif: nous recommandons d'ajouter un appareil de protection 2A Min. - 5A Max., facilement accessible dans le circuit électrique de l'immeuble. Un appareil de protection à circuit 5A peut alimenter 2 unités ML630R placés l'un sur l'autre en étagères.
13. L'équipement doit être connecté à un système d'alimentation mis à la terre correctement.
14. Tout équipement à proximité immédiate doit avoir la même mise à la terre et ne doit pas avoir une mise à la terre ailleurs.
15. Ne placez pas un appareil déconnecté dans le circuit mis à la terre entre la source d'alimentation DC et la connexion au circuit mis à la terre.

Prévention des décharges électrostatiques (ESD) Dommages

1. Lorsque vous travaillez avec des composants électroniques, portez un bracelet antistatique mis à la terre pour décharger l'électricité statique de votre corps en conformité avec les normes approuvées.
2. Ne pas utiliser d'appareils capables de générer ou maintenir une charge statique dans la zone de travail où vous installez ou supprimez des composants électroniques. Éviter de manipuler les composants électroniques dans des endroits qui ont un sol capable de générer une charge statique.
3. Ne pas faire glisser les composants électroniques sur une surface quelconque. Ne touchez pas les broches du connecteur exposés. Manipulez les composants électroniques aussi peu que possible.
4. Transporter et stocker les composants électroniques dans un sac ou conteneur antistatique approuvé.

Avis aux consommateurs

Le produit Actelis acheté est soumis aux dispositions de la directive 2002/96/CE du Parlement européen et du Conseil de l'Union européenne sur les déchets d'équipements électriques et électroniques (DEEE) et, dans les juridictions qui adoptent cette directive, est marqué comme mis sur le marché après le 13 août 2005, et ne doit pas être jeté avec les déchets municipaux non triés. Veuillez utiliser vos installations de collecte DEEE locales pour la disposition de ce produit et sinon observer toutes les exigences applicable.

Allgemeine Sicherheitshinweise

1. Lesen Sie alle Warnhinweise und Anweisungen zu diesem Produkt, welche in diesem Handbuch hervorgehoben sind.
2. Installation oder Austausch von Baugruppen muss von qualifiziertem Personal durchgeführt werden.
3. Bevor das Gerät eingeschaltet oder eine Baugruppe eingesetzt wird, die korrekte Erdung überprüfen.
4. Die Switche nutzen eine externe Gleichspannungsquelle. Vermeiden Sie den Kontakt mit freigelegten Anschlüssen, Kabeln oder Komponenten, wenn die Spannung eingeschaltet ist.
5. Die Switche **nicht** in Betrieb nehmen, wenn Frontplatten entfernt wurden, eine mechanische Beschädigung oder ein Defekt der elektronischen Bauteile vermutet wird.
6. Die Switche **nicht** in einer nassen, feuchten oder explosiven Umgebung in Betrieb nehmen.
7. Oberflächen sind trocken und sauber zu halten.
8. Stellen Sie die Lüftung sicher.
9. Beachten Sie die Angaben und Hinweise auf dem Produkt. Nur die für dieses Produkt empfohlenen Sicherungen verwenden. Bevor Sie Anschlüsse an die Switche durchführen, bitte sorgfältig die Hinweise in den Benutzerhandbüchern durchlesen.
10. Viele der an die Switche angeschlossenen Kabel, werden von Actelis Networks geliefert. Kabel welche nicht von Actelis Networks geliefert werden, müßen den sonstigen Sicherheitsvorschriften entsprechen. Um Risiken zu vermeiden, sollten Kabel UL oder CSA zertifiziert sein.
11. Die Switche müssen entsprechend den Ländervorgaben für elektrische Anlagen installiert werden.
12. Überstromschutz: Es wird empfohlen den Stromkreis mit mindestens 2A bis maximal 5A abzusichern. Ein Stromkreis mit 5A Absicherung kann typischerweise zwei ML630R Switche speisen.
13. Die Geräte müssen an eine richtig geerdete Speisungsquelle angeschlossen werden.
14. Benachbarte Geräte sind in der gleichen Weise zu Erden und nicht auf anderem Wege.
15. Ein Abschaltmechanismus in dem Erdungsanschluss zwischen der Gleichspannungsquelle und der Erdung ist nicht zulässig.

Schutz vor elektrostatischer Entladung

1. Beim Arbeiten mit elektronischen Komponenten, muss ein entsprechendes Erdungsband getragen warden, um elektrostatische Spannungen vom Körper abzuleiten entsprechend der zugelassenen Standards.
2. Nutzen Sie keine Geräte in dem Arbeitsbereich, welche eine elektrostatische Ladung hervorrufen können.

   Vermeiden Sie das Hantieren der Switche in elektrostatisch kritischen Fussboden -oder Tischumgebungen.
3. Vermeiden Sie die Switche auf rutschige Oberflächen zu stellen.

4. Transportieren Sie die Geräte nur in passenden antistatischen Verpackungen.

Hinweis für Endverbraucher

Das gekaufte Actelis Produkt unterliegt der Richtlinie 2002/96 / EG des Europäischen Parlaments und des Rates der Europäischen Union über Elektro- und Elektronik-Altgeräte (WEEE). Es wurde unter Anwendung der Direktive nach dem 13. August 2005 auf den Markt gebracht und sollte nicht als Haushaltsmüll entsorgt werden. Bitte nutzen Sie Ihre lokale WEEE-Sammelstelle für die Entsorgung des Produkts und beachten Sie auch alle sonstigen Vorschriften.

About This Manual

This section provides a guide on how to use the manual effectively. The manual contains information needed to install, configure, and operate ML630R Series units. The summary of this manual is as follows:

Chapter 1: Overview

Describes ML630R Series in several applications.

Chapter 2: Specifications

Describes the features, specifications and applications of ML630R Series.

Chapter 3: Interfaces

Introduces all the interfaces, including front panel and rear panel of ML630R Series.

Chapter 4: Installation

Assists the user in installing and verifying the ML630R Series step-by-step.

Chapter 5: Web operation

Gives a description of the Web Interface.

Chapter 6: CLI Operation of

Gives a description of the CLI (Common Line Interface).

Appendix A: Pin Assignment

The description of pin assignments

Symbols Used in This Manual

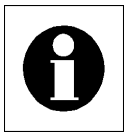
3 types of symbols are used throughout this manual. These symbols are used to advise the users when a special condition arises, such as a safety or operational hazard, or to present extra information to the users. These symbols are explained below:

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.

CONTENTS

FIGURES

TABLES

I. Overview

This chapter begins with a general description of the ML630R Series. The chapter then describes examples of several applications.

1. Overview

DSL (Digital Subscriber Loop) technologies increase the bandwidth capacity of existing ubiquitous telephone line (the local copper loops). G.SHDSL is designed for business applications, where high speed is required in both transmission directions. It provides symmetrical data rates of 192Kbps to 15Mbps in 1 pair with a transmission distance up to 3km/10Kft using SHDSL technology. The data rates will be increased to 30.464Mbps in 2 pair links and 60.932Mbps in 4 pair links. The speeds 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 ML630R is G.SHDSL.bis transmission equipment that uses EFM/ATM frames to enable Ethernet extension. ML630R provides local loopback functions thereby enabling system configuration, testing, performance and alarm monitoring of the DSL link. This feature is very convenient for network testing and maintenance.

II. Specification

To provide understanding of the ML630R Series, this chapter starts with its main features. The chapter then continues to present the SHDSL.bis interface, the network side interface, timing and synchronization, OAM (Operation, Administration and Maintenance) and technical specifications.

2. Main Features

Listed below are the main features of the ML630R Series:

- ML630R series supports EFM and ATM mode.
- Point-to-point G.SHDSL.bis/Ethernet copper lines.
- 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 single pair copper wire, and up to 15Mbps per copper pair for shorter distances.
- 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 1 pair, n is 6 to 178 in 2 pairs, and n is 12 to 356 in 4 pairs.
- Support EFM on extended mode for payload rates up to 60Mbps in 4 pairs.
- 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 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 routing.
- 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.

3. 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 via 1 pairs, 2 pairss or 4 pairss twisted pair.
- Port enabled / disabled configurable.
- Line Protection: meet ITU-T K.21 requirements.

4. Network Side Interface

4.1. 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 devices
- 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)

5. OAM

OAM (Operation, Administration and Maintenance) of the ML630R 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 lost of CPE mode.

6. Technical Specifications

The following table gives the technical specifications of the ML630R Series.

Table 2-1 Technical Specifications of the ML630R Series

DSL	
Modulation	TC-PAM 4/8/16/32/64/128
Mode	Full duplex with echo cancellation
Number of pairs	Two pairs on ML632R Four pairs on ML634R
Bandwidth	N*64+8K (N=3~238) up to 15.232Mbps (1 pair), (N=6~576) 30.464Mbps (2 pairs), (N=12~1152) 60.928Mbps (4 pairs)
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 bit 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 Support 4 LAN ports	
Power Requirement		
Input	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	
Power Consumption	< 7 Watt	
Environments		
Temperature	Operating	0 ~ +50℃
	Storage	-20 ~ +70℃
Humidity	Operating 90% non-condensing Storage 95% non-condensing	

III. Interfaces

In this chapter, the ML630R interfaces will be discussed, and the the front & real panels.

EFM/ ATM models					
Model	G.SHDSL	LAN	G.8032	DIP SW	Craft
ML632R	2 pairs	4	LAN	●	DB-9
ML634R	4 pairs	4	LAN	●	DB-9

7. Front Panel of ML630R series

The front panel of ML630R, as illustrated in Figure 3-1, contains four main sections, management (craft) port, status indicators, DIP switch and buttons. Via the front panel of ML630R Series, users can perform the functions as listed below:

- Displaying system status
- Resetting the device and the alarm LED
- Managing ML630R 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 ML630R series

7.1. Status Indicators

The status indicators of the ML630R are depicted in table below.

There are six classes of LEDs on ML630R, which are PWR, TST, CPE, ALM, MLP1-4 and ETH1-4. These LEDs display the system status.

Table 3-1 Indicators on Front Panel of ML630R 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
MLP1-4	DSL Link	Warning	DSL Alarm	DSL handshake	Not Used
ETH1-4	Ethernet Link			Ethernet active	Link Down

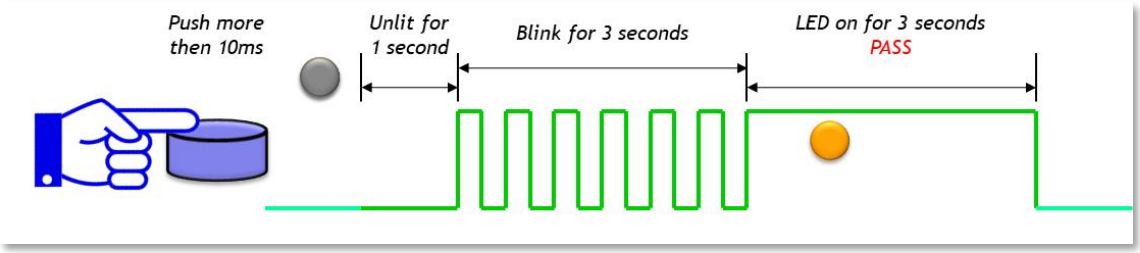
****The front panel indicators on the WEB UI may show the 100M full duplex mode of LAN in yellow**

7.2. The RST Button

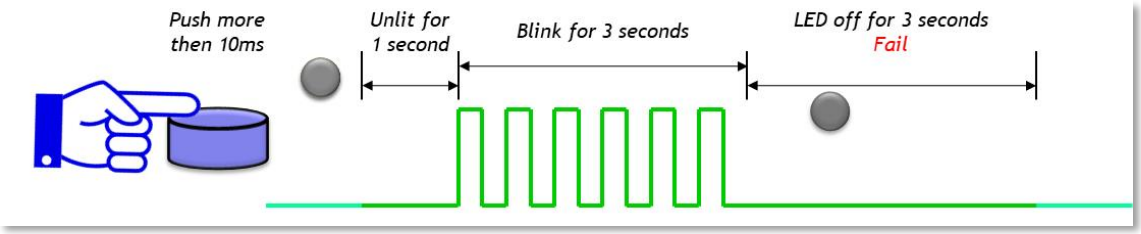
There is one “RST” Reset button to manually reset the device. Pushing the RST (reset) button for over **5 seconds** will manually reset the device back to its factory default setting; including login username, password, IP address and all configuration.

7.3. The TST Button

This function of the TST button is only for the in-service-loop health detection of DSL link between CO and CPE modems. Pushing the TST (test) button for over 10ms will perform the loop test which tests the link status of all DSL loops.



All loops connected OK: the TST LED **is lit for 3 seconds** after the test. It turns OFF for one second and then blinks for 3 seconds and finally **lights for 3 seconds**.



Any loop links fail: The TST LED **goes OFF after test**. It goes OFF for one second, then blinks for 3 seconds and finally **stays off for 3 seconds**.

8. Rear Panel

The figure below illustrates the rear panel of the ML630R Series. Users may connect the ML630R Series to other devices or equipment via these interfaces.

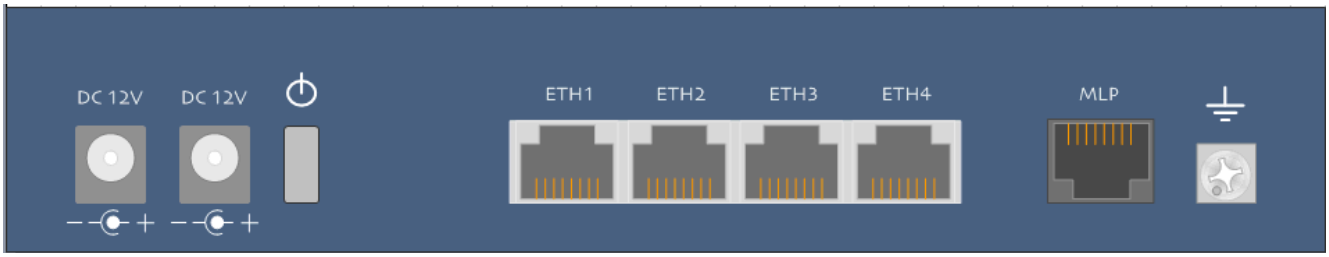


Figure 3-2 Rear Panel of ML630R Series (12VDC)

The following connectors/devices appear on the rear panel of the ML630R Series.

- Power On/Off: The ML630R Series' power switch
- Power connectors: Redundant power for a DC power cable coming from an AC/DC adapter
- Ground line *1
- ETH: Ethernet ports for RJ-45 connector
- MLP (Modem Line Port): RJ-45 jack for SHDSL link (General or special converter cable)
- DC IN: 12Vdc + 36~72Vdc or 12Vdc + 12Vdc

IV. Installation

This chapter describes the installation process for the ML630R. It begins with a checklist for unpacking the shipping package.

9. Unpacking

ML630R Series shipping package includes the following items:

- ML630R Series standalone unit
- AC to DC Power adapter
- G.SHDSL cable (RJ45-RJ45)
- Junction Box (from RJ45 to 8 wires)

10. Site Requirements

10.1. Site Selection

Install the device in a clean area that is free from environmental 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 the rear for cable clearance. Position the device so you can easily see the front panel.

10.2. AC/DC Electrical Outlet Connection

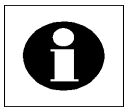
The ML630R Series with 12VDC input should be installed with the provided AC/DC power adapter which has an AC input range of 100 to 240VAC at a frequency of 50Hz to 60Hz. For redundancy, a second AC/DC adapter (not supplied with the ML630R) can be plugged into the second 12VDC plug.

10.3. Grounding

Make sure the electrical power 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 from lightning is high, disconnect the device from the transmission line at the rear panel when it is not in use.

11. Cable Connection

11.1. Connecting the IP Network via Ethernet

On the ML630R standard unit, 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 is 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 (UTP) cable or shielded twisted-pair cable is used. Two twisted pairs are used for separating Rx (receive) and Tx (transmit). The Fast Ethernet port is backward compatible with traditional 10Base-T Ethernet. ML630R series can automatically detect whether it is connected to a 10Base-T or 100Base-T Network.

11.2. Connecting the Terminal

The console port connector labeled “CRAFT” on the front panel of ML630R is provided for connection to an external ANSI or VT-100 compatible terminal to perform local configuration of ML630R.

Craft port Speed & Data format: 115,200bps, none parity, 8 data bits, 1 stop bit, and no flow control.

Table 4-2 Craft Port connections 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

Craft port connections in DB9 connector

11.3. Connecting the DSL on Devices

ML630R series provides 1, 2, or 4 pairs connection on the DSL port.

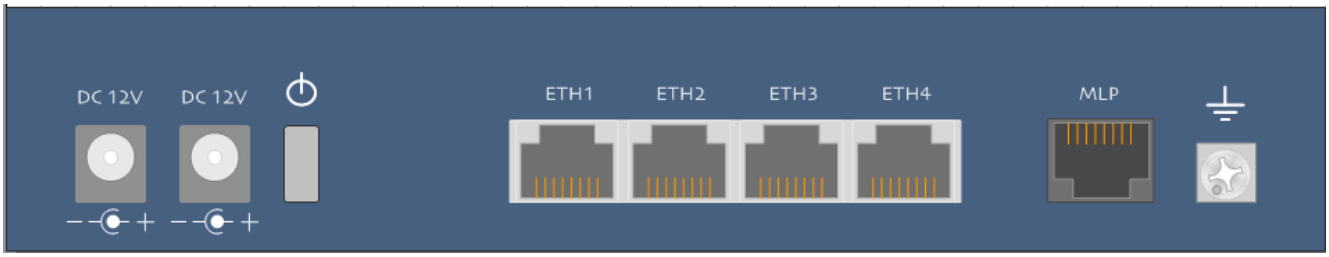


Figure 4-1 ML630R Series DSL Interface

The DSL interface uses the RJ-45 MLP (Modem Line Port) connector for 1, 2 or 4 DSL pairs, with the pin configuration as shown in Appendix A.2.

12. Quick Setup

ML630R Series has a “DIP Switch” on the front panel for quick setup. It provides users a quick method to configure the device for CO (Central Office) or CPE (Customer Premises Equipment) operation.

Figure 4-2 ML630R Series DIP Switch

- Keep local DIP switches to all **OFF** (Default CPE mode).
- Change the remote unit **DIP-1** switch to **ON** (For CO mode).
- Connect the provided RJ45-RJ45 cable to the DSL loops (MLP connector) or connect wires directly to the MLP connector as described in A.2.
- Connect the junction box to the other end of the RJ45 cable
- Connect the DSL pairs to the junction box according to the pinout described in Appendix A.2.
- Connect the AC/DC adapter to the DC power jack and plug it in to a power socket to start working.

Caution:

When turning **DIP-2** to **ON,** the Ser2Net function may affect the console functionality. Please remember to use a static IP address for WEB management, in case either Console or Ser2Net is used.

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

V. Web Interface

*In this chapter, the user will be introduced to the web interface of ML630R Series. The chapter starts with an overview of device's web interface. In additional, each main menu item of the web interface, such as Configuration, Maintenance and Status will be explained thoroughly. The following descriptions are based on the ML630R with firmware version **v1.371**.*

13. Overview

Users should initially 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 management IP address is http://192.168.0.1.

ML630R supports the following WEB browsers:

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

14. Login Page

In this page, users need to enter the correct user name & password. There are three default 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

15. Status

The local status can be obtained in this section.

15.1. Local Status

For the 4-pairs model (ML634R), there are four loop indexes: MLP1, MLP2, MLP3 and MLP4. Thus, MLP1 and MLP2 are available for the 2-pairs model (ML632R), and MLP1 is only available for the 1-pair model (ML631R).

The following information tabs show Line Status, Current Alarm and Current Performance.

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

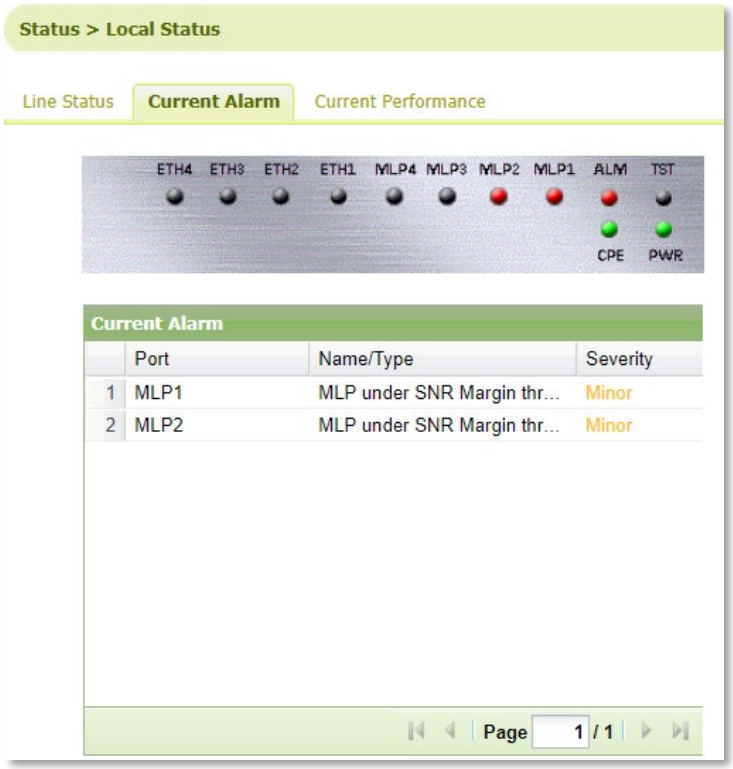


Figure 5-3 Current Alarm

The following parameters are shown in "**Line Status**":

- **MLP 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/ HDLC/ 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.

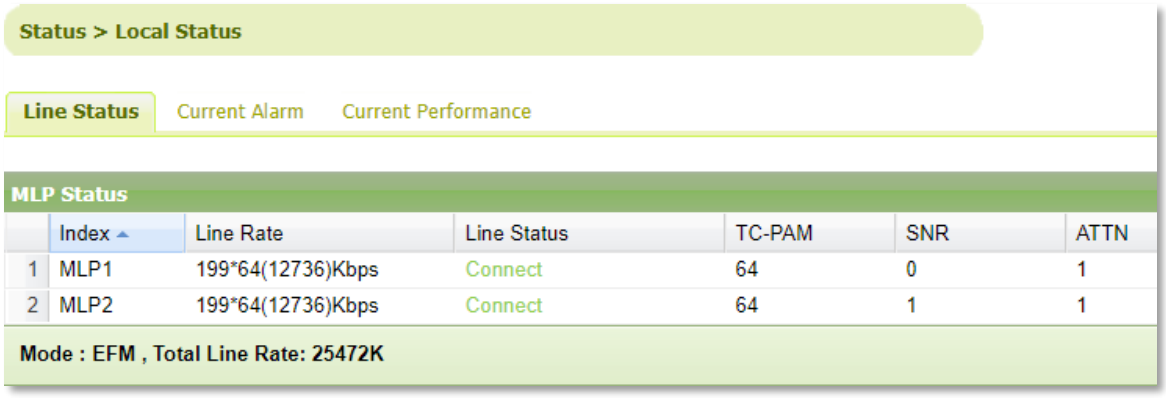


Figure 5-4 Line Status

Note: For the 4-pairs model (ML634R), the total speed is the summary of all the loops' Line Rate.

For instance, if two loops are at speed (199 x 64kbps = 12736kbps), the total speed of DSL trunk is 12736 + 12736 = 25472kbps.

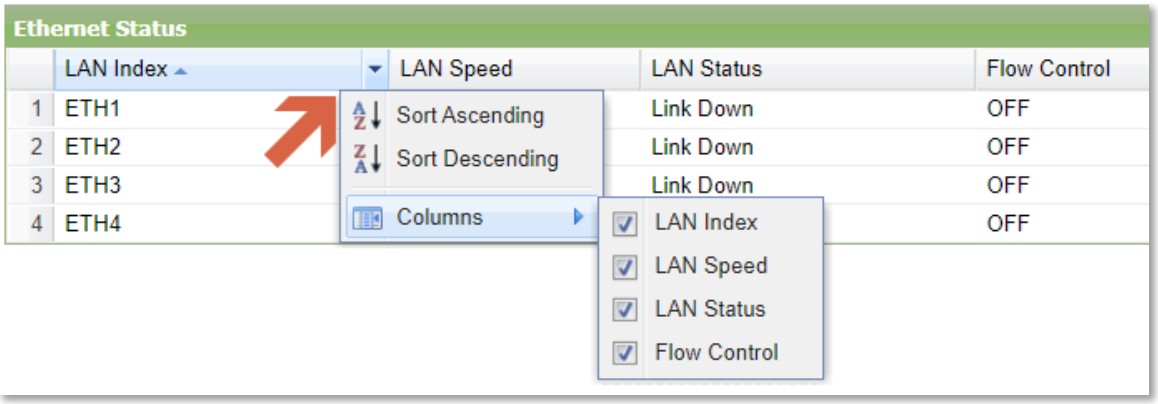


Figure 5-5 Ethernet Status

By click on index icon, the sorting rule will show and help to display in different field of form. The Ethernet Status can read its Speed, Status or Flow Control by the index on or off.

- **Current Performance:** shows the current G.SHDSL error performance statistics in 15 minutes and 1 Day duration.
- **LOSW:** Lost of Sync Word seconds.
- **ES:** Error Seconds
- **SES:** Severely Error Seconds
- **UAS:** Unavailable Seconds

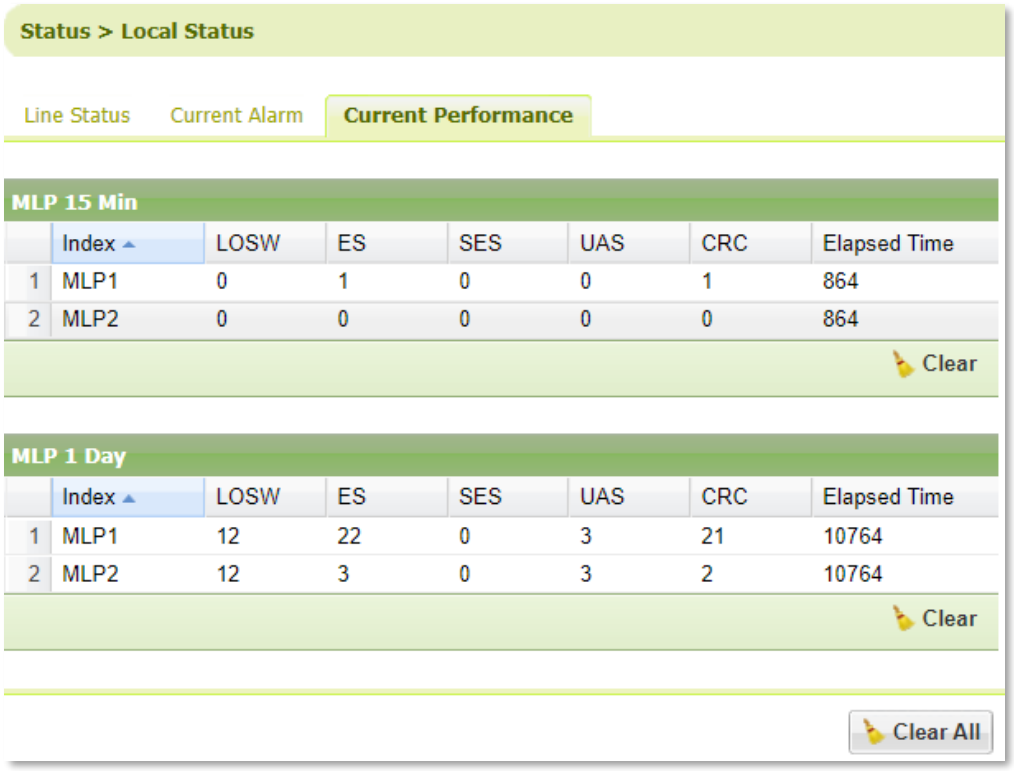


Figure 5-6 ML630R Current Performance

16. Configuration

ML630R Series supports Local configuration.

16.1. Load Local Profile

There are two default profiles in ML630R for users to select, as shown in the Figure below. The default profile is CPE mode. If a pair of ML630R are connected via DSL in the field, users can select the one profile for CO mode (profile 1) and another one to CPE mode (profile 2) for quick setup.

Factory Profile

Choose	Index	Mode	Interface				Clock	Line Probe	Boot	Default
			Ethernet	E1	DataPort	G.SHDSL				
◉	1	CPE	89			89(Auto)	Recovery from DSL	ON		✔
○	2	CO	89			89(Auto)	Internal	ON		

User Profile

Choose	Name	Mode	Interface				Clock	Line Probe	Boot	Action
			Ethernet	E1	DataPort	G.SHDSL				
○	Profile	CPE	Auto	0	0(V.35)	89(2w)	Recovery from DSL	ON	✔	

Figure 5-7 SHDSL Load Local/Remote Profile*

The operator may save and restore their “User Profile” for keeping all modified configurations. These “User Profiles” can be saved and restored in local storage as a file for easy backup and restoring to either the same or another ML630R device.

In the above example, the total line rate can reach up to 89 x 64kbps (G.SHDSL = 89).

16.2. Local Setting

There are 3 modes users can select: EFM, ATM and HDLC. However, HDLC is not relevant for the ML630R.

- **EFM mode:** Users can modify the G.SHDSL and Ethernet parameters. The clock source is automatically selected, and 15.232Mbps per pair can be configured in G.SHDSL connection using the extended mode.
- **ATM mode:** Users can modify the G.SHDSL, Ethernet & ATM parameters. On the ATM page, General Setup includes basic ATM protocols and ATM Parameters for VID, VPI and VCI.

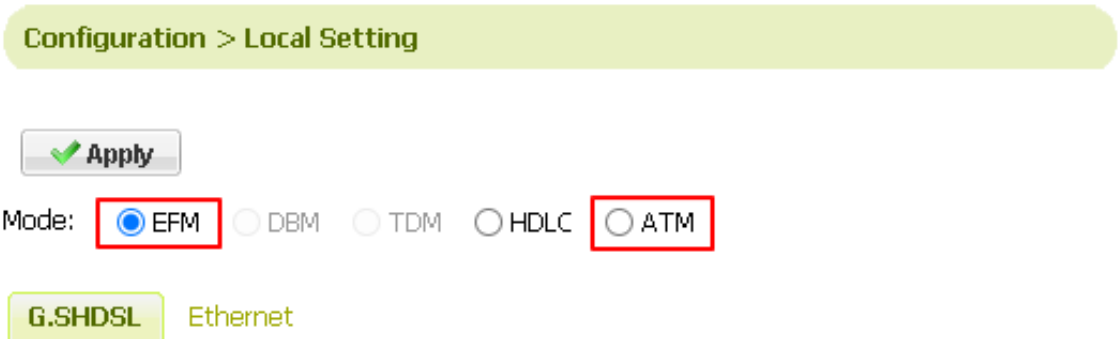


Figure 5-8 Local/Remote Setting in Different Mode*

16.2.1. G.SHDSL Setting in EFM mode

- **G.SHDSL configuration:** Some functionality can only be configured by the ML630R in CO mode, for example, "**Line Rate**" and "**Power Backoff**" can not be configured in **CPE** mode.
- **Wire Mode**: ML630R Series support 2W, 4W, 8W and Auto.
- **Power Back off, PBO Value:**

Power back off is used to reduce the data transmission power over the loop length. When it is set to "Auto", it dynamically reduces the power level in order to eliminate the potential for interference with the digital local loop resulting from near-end crosstalk. Only the ML630R 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 configured from 0 to 31 dB attenuation.

- **Line Probe:**

When Line Probe is set to ON, the device adjusts the DSL line data rate automatically according to the SNR Margin. The DSL line quality is represented by SNR (Signal Noise Ratio). The higher the SNR value, the better the DSL line quality. When the SNR value is very low, the DSL line might become unstable and disconnect.

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

If the actual SNR value is lower than the SNR margin value, the device will decrease the line rate to prevent the SNR value from dropping and to keep the DSL link up. However, users should be aware of that there is a relationship between the line rate and loop length. As the DSL loop length increases, the DSL line rate decreases, and vice versa.

- **Extended Mode:** In EFM mode, the ITU-T G.991.2 standard supports TC-PAM4/ 8/ 16/ 32 modes. In addition, the ML630R supports TC-PAM64/128 mode

(G.SHDSL.bis - G.991.2 annex F&G) to reach higher data rates. TC-PAM 128 supports up to 238 x 64Kbps = 15Mbps.

- **Miscellaneous:** For the ML630R Series, the setting is fixed. CO side is "**Internal**", and CPE side is "**Recovery from DSL**".
- **Threshold**: For better troubleshooting, users can choose the ATTN, SNR and CRC thresholds beyond which alarm traps will be generated.

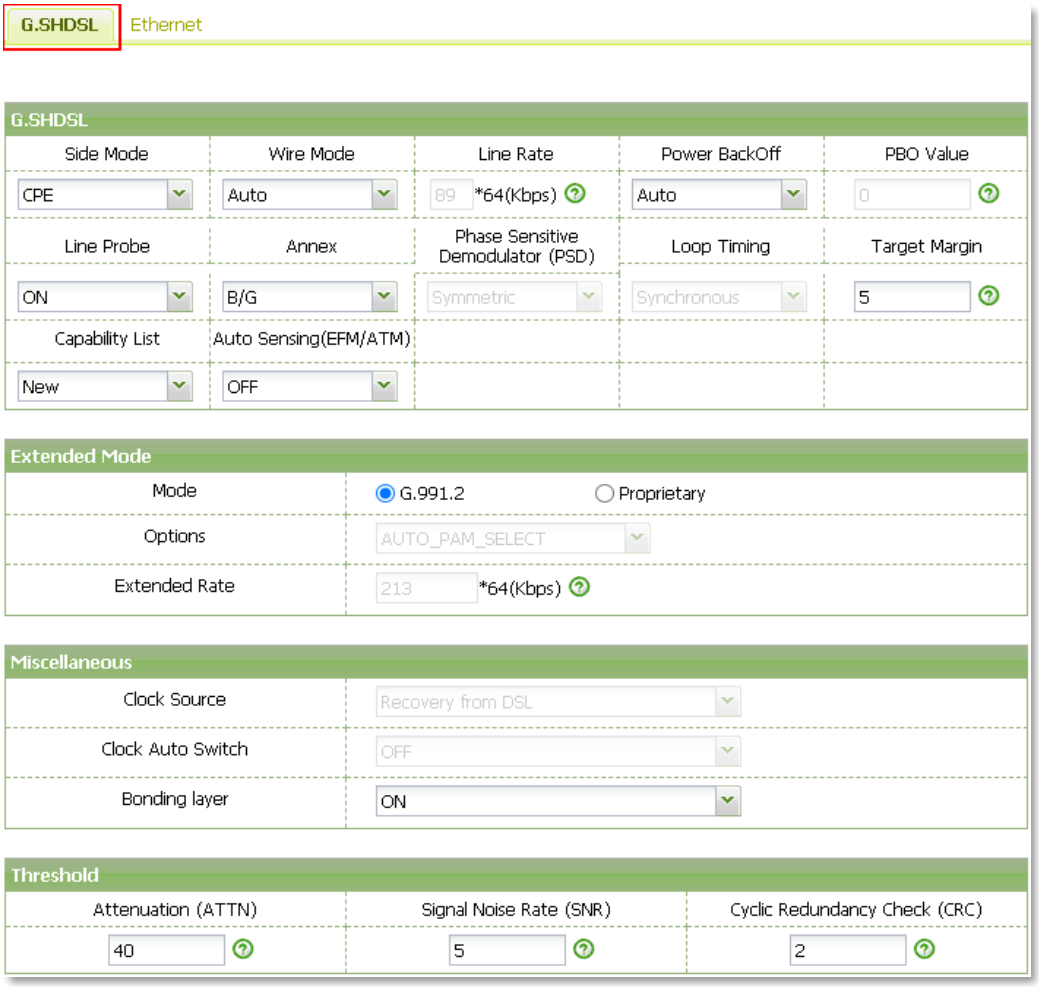


Figure 5-9 Local/Remote Setting in G.SHDSL*

- **Admin:** The LAN port will be turned off if users configure it to "**OFF**".
- **Speed:** The default speed is "Auto", users can select 10-Half, 10-Full, 100-Half or 100-Full.
- **Alarm Switch:** If "**Alarm Switch**" if turned on, then Ethernet interface alarms will be reported.
- **Flow Control:** The default Flow Control is "**ON**". Users can select "**OFF**" to disable.
- **Ingress:** By default, there is no Ingress limit. Users can limit the input traffic from 64Kbps to 50Mbps.
- **Egress:** By default, there is no Egress limit. Users can limit the output traffic from 64Kbps to 50Mbps.

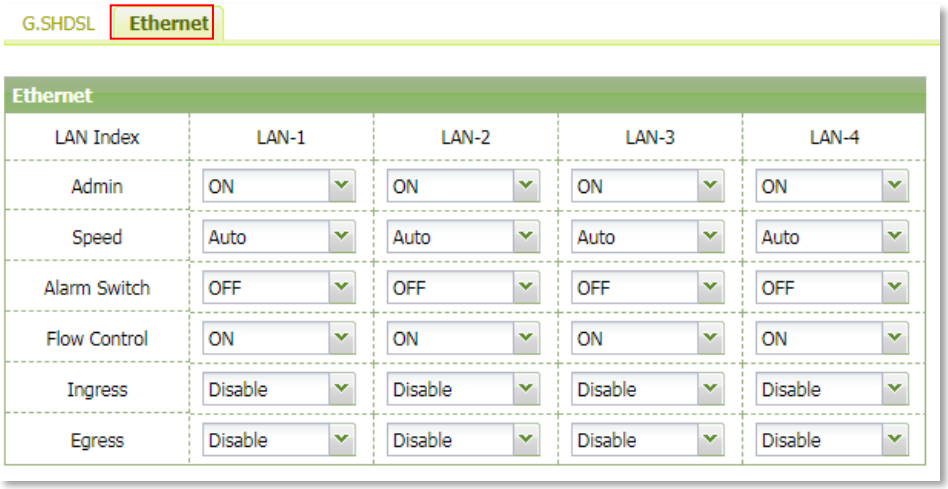


Figure 5-10 Local/Remote setting in Ethernet*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

16.2.2. 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" which identifies the protocol that the 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**". If there is a packet mismatch with the 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 VLAN PVID range is from 1 to 4095.

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

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

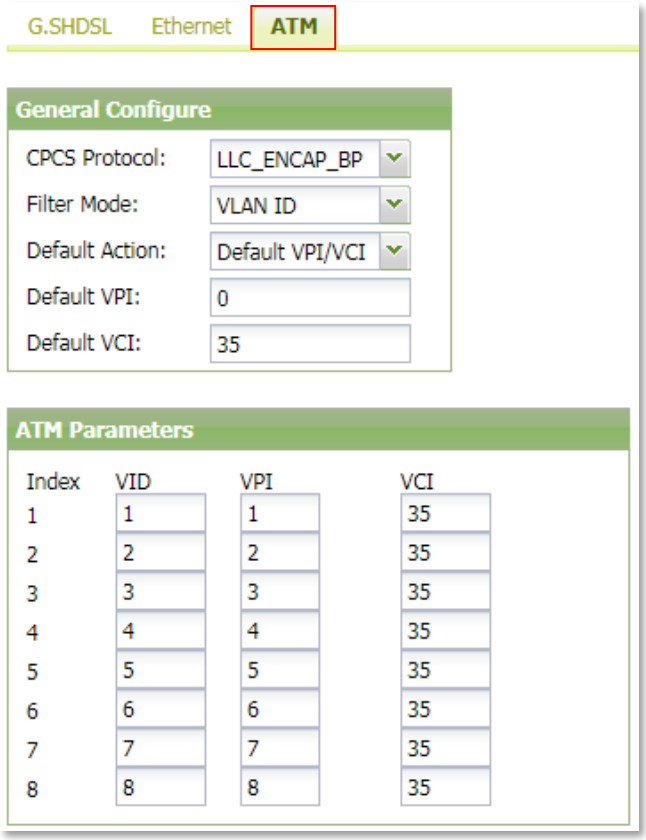


Figure 5-11 Local/Remote setting in ATM*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

16.3. User Management

In this page, there are three default privileges for different users' priorities. To improve security in the ML630R, remember to configure the correct security mechanism when creating new accounts.

- Administrator – has the highest operation privilege to control all functionality allowing adding, deleting or modification of all accounts.
- Operator - privilege level allowing control of all functions, except creating or deleting any accounts.
- Monitor – read-only information functionality.

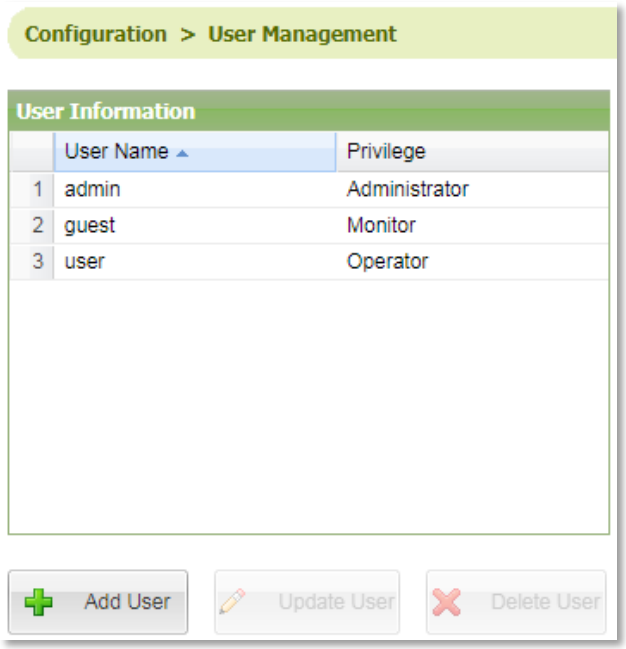


Figure 5-12 User Management

16.4. 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 flexible allowing for site customization and future development features, and it uses TCP to ensure reliable delivery. The protocol allows the TACACS+ client to request very specific access control and allows the daemon to respond to each component of that request.

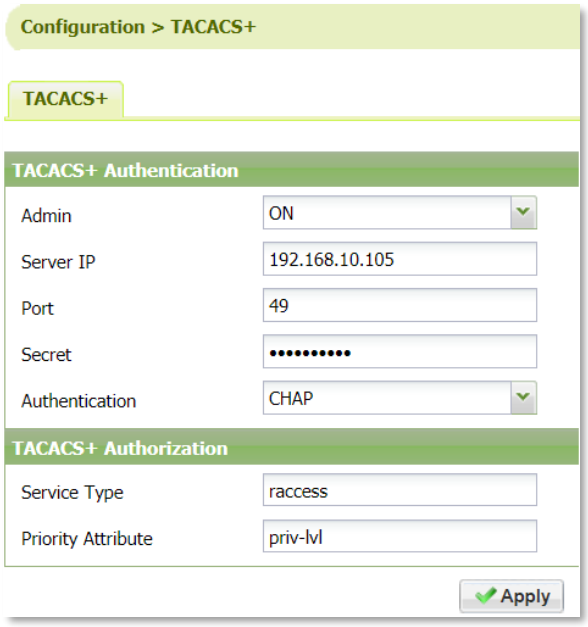


Figure 5-13 TACACS+ setup

- **Admin**: The default parameter is “OFF”. Switch it to “On” to start the TACACS+ authentication.
- **Server IP**: The IP address of the TACACS+ server.
- **Port:** The default TACACS+ TCP port is 49.
- **Secret**: The phrase string to be used for the authentication key.
- **Authentication:** The authentication type of the phrase string 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. The default text is “priv-lvl”.

16.5. Date & Time (Local/Remote*)

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

There are two ways to configure the device. Either by communicating with an SNTP server for retrieving the time, or to set the time manually. The [Daylight saving time] function moves the clock back by one hour.

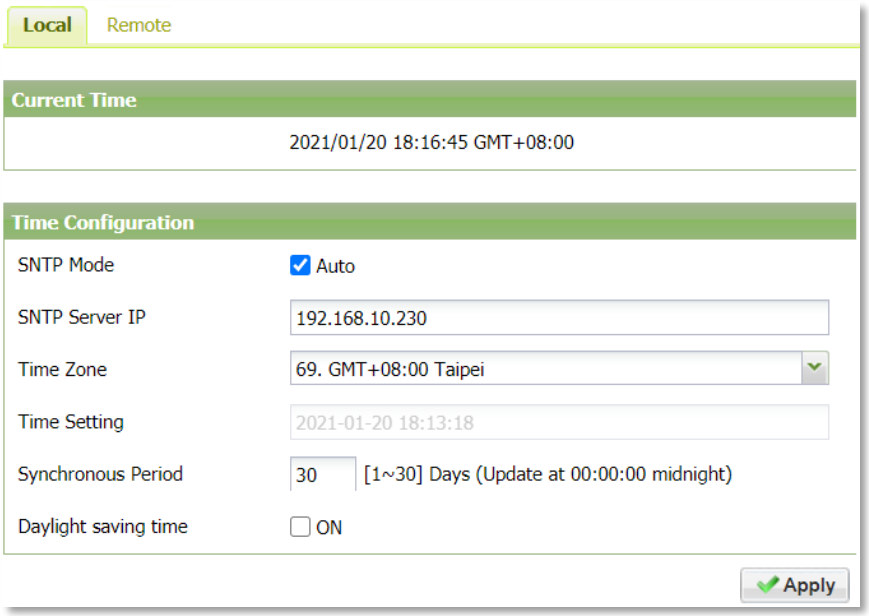


Figure 5-14 Local/Remote Date & Time*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

16.6. General Setup (Local/Remote*)

The IP configuration can only be configured in this menu when the ML630R is configured for **Bridge** application. The menu includes two main items, "**System IP**" and "**Link Security**".

System IP: The management IP address of this device. Note that after changing the system IP address (after the operator clicks the apply button), the change will only be applied after the unit is powered down and powered up again. Remember to save the configuration after configuring the system IP.

Link Security: The link security function is only relevant when the ML630R is used both as a CO and a CPE. 6 fixed digital numbers (0-9) need to be configured. When 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.

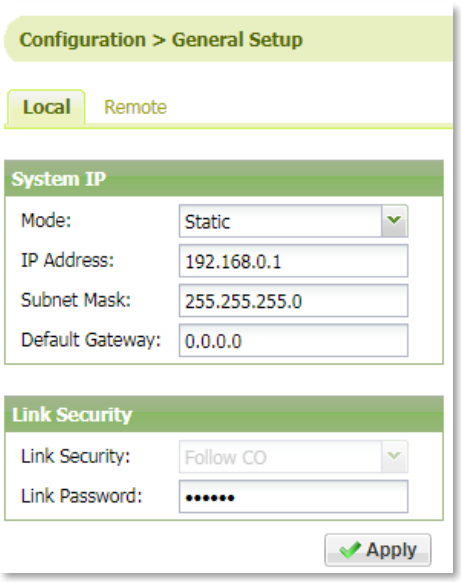


Figure 5-15 Local/Remote General Setup*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

Note:

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

16.7. DHCP Server

- **Configuration**: The default tab is configuration. Users can change the DHCP mode from OFF to DHCP server or DHCP relay (The server & client need to be in the same network). If the operator configures the SHDSL modem as DHCP server, the most important settings are "**Start IP**" and "**End IP**" which should be in the same network segment as the device's LAN. Other requirements, such as "**Lease time**", "**Gateway**", "**NTP Server**" or "**DNS IP**" should match the operator's environment.

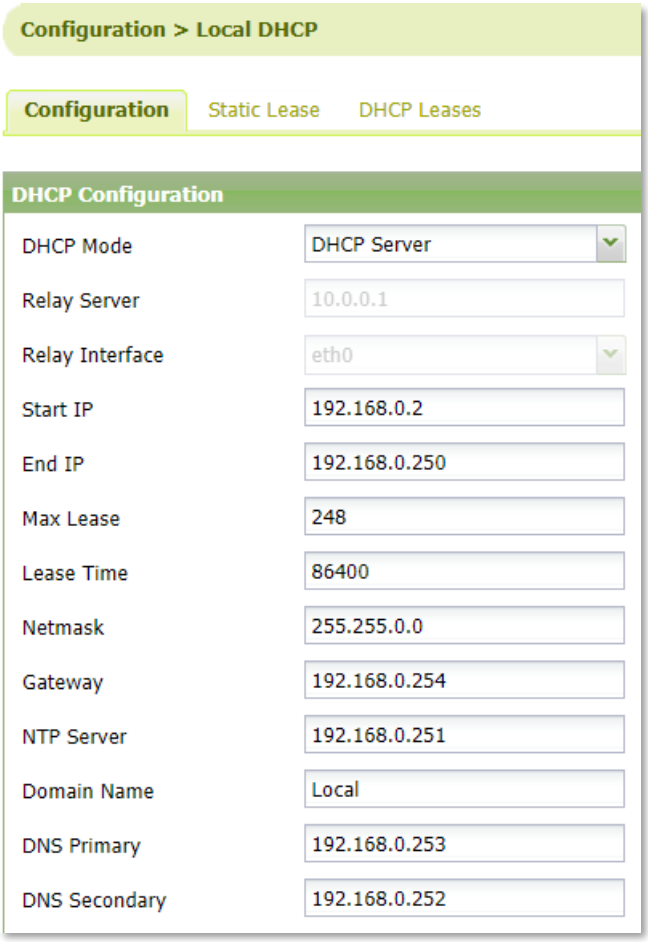


Figure 5-16 DHCP Server Configuration

- **Static Lease:** This function works when DHCP server is configured. Operators assign a specified IP to a specified DHCP client. The method of identification is to check the DHCP client via the MAC address. Users also have to ensure that the specified IP is within the range of "**Start IP**" and "**End IP**".
- **DHCP Leases:** The tab includes IP, MAC address and Expire time. When the SHDSL modem acts as a DHCP server, the device will record all DHCP clients.

16.8. IPv6 (Local/Remote*)

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol. IPv6 developed by the IETF to deal with the long-anticipated problem of IPv4 address exhaustion. The ML630R series follows the future trends and multi-application. IPv6 packets can be transmitted through the DSL, and the device can also be managed 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 enable IPv6.
- **IP Address:** The management IPv6 address of this device. The setting changes immediately after the operator clicks the "**Apply**" button, but this change will not be saved and implemented until the ML630R is powered down and up again. Operators must click "**SAVE**" to save the IPv6 address. The format of this item is

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

  After clicking 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 allow the device to access other networks via the default route.

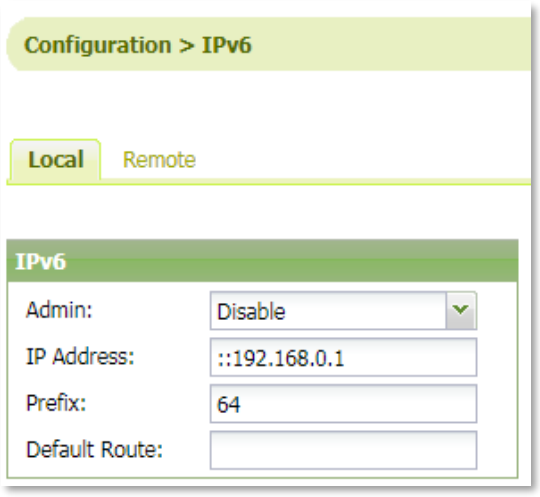


Figure 5-17 Local/Remote IPv6*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

16.9. SNMP & SysLog

To set up the destination IP address for sending traps or syslog, users can go to

the [Trap IP] submenu. Input and activate the desired IP address / Domain name. The setting value will activate by pressing the “Apply” button. When the trap or syslog IP is configured, the ML630R alarm information will send to these destination addresses. The trap IP address is usually the address of the SNMP network management system.

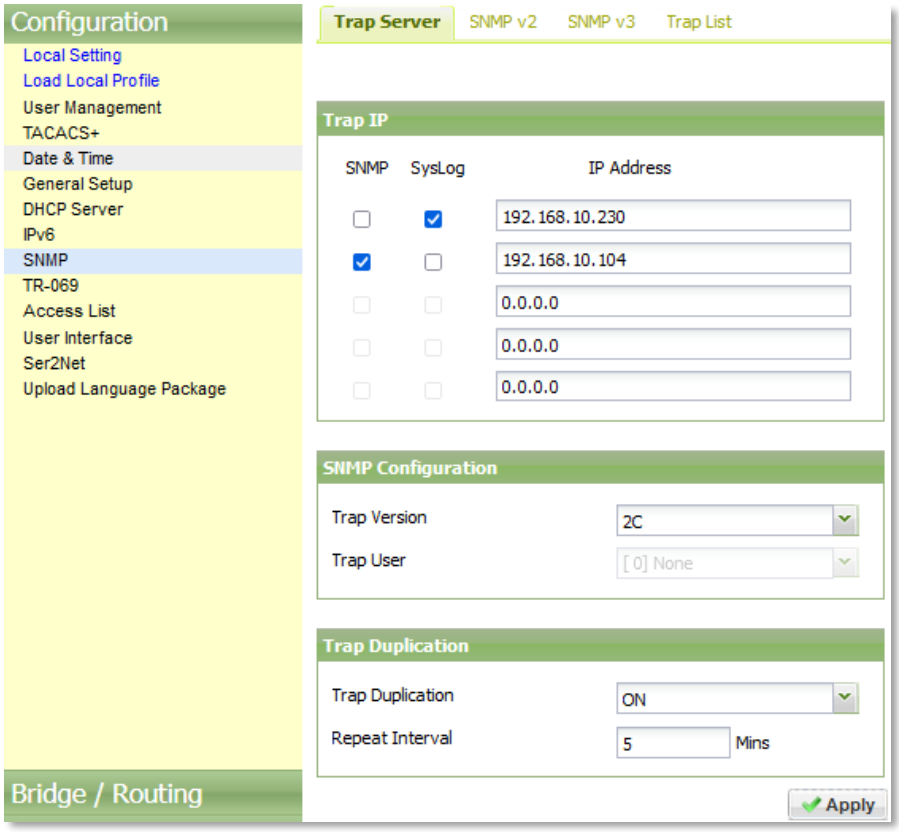


Figure 5-18 SNMP Trap Server

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

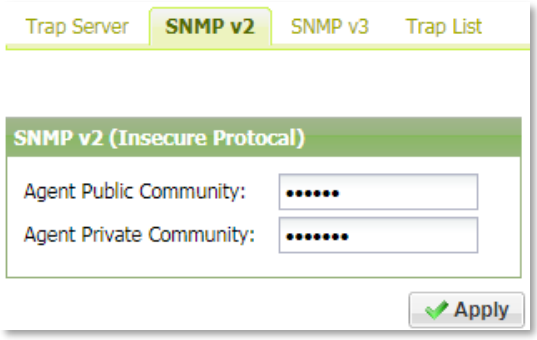


Figure 5-19 SNMP v2 Setup

To ensure the maximum security level of SNMPv3, it is recommended that users configure the privilege to “Auth & Pri”. In other parameters, MD5 is more secure than SHA, and AES is more secure than DES.

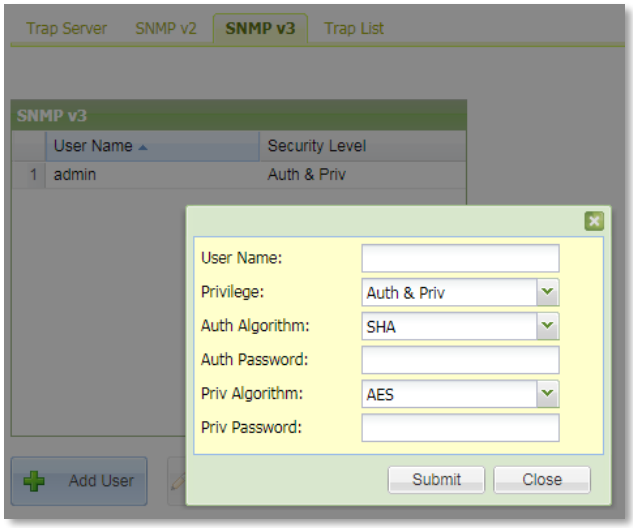


Figure 5-20 SNMP v3 Setup

Users can change the severity in the trap list. The configurable severity levels are critical, major, minor and warning. Remember to click the "**Apply**" button after configuring.

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 5-21 Trap List

16.10. TR-069

The ML630R supports the TR-069 protocol, which acts as an ACS client. All parameters in this form are designed to communicate with ACS server. In order to pass the ACS certification successfully, ensure that 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 "**Enable**" is to enable TR-069.
- **CPE Port:** ACS client port number
- **Connection Request User Name**: Define the ML630R's user name. The device has its own authentication, to allow ACS server access.
- **Connection Request Password:** Define the ML630R's password.
- **ACS URL**: The URL of the ACS server.
- **Login ACS User Name**: Refer to the ACS server's user name.
- **Login ACS Password**: Refer to the ACS server's password.
- **Periodic Inform**: ML630R will request the ACS server to keep communicating at regular intervals.
- **Periodic Interval**: The unit of time is seconds.

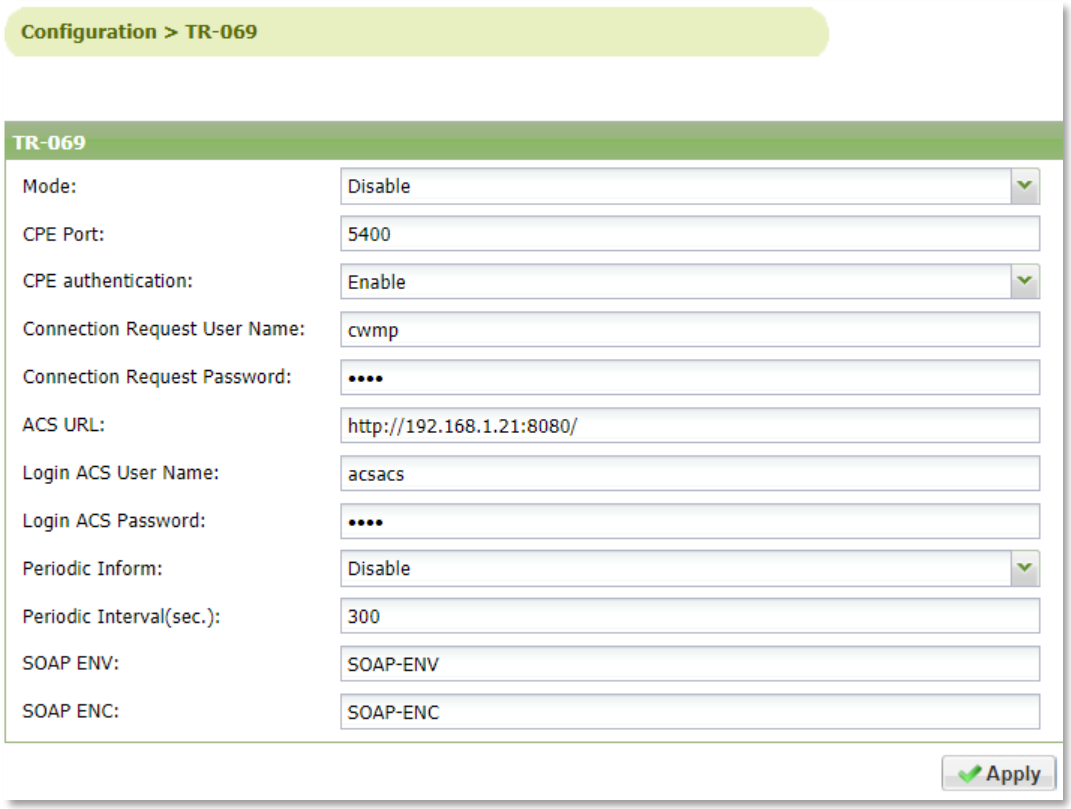


Figure 5-22 The TR-069 parameters

16.11. Access List

In order to filter data packets, ML630R needs to set a series of rules for identifying what needs to be filtered. The device supports ACL "**White List**" mode and "**Normal**" mode.

- **White List:** Any data matching the rules to pass through the devices, otherwise, the packet will be dropped;
- **Normal:** Any data matching all the 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 the ingress port to perform the ACL function.
- **Physical Port (Egress):** Select the egress port to perform the ACL function.
- **ETH Type:** Table 5-2 lists some EtherType examples for reference

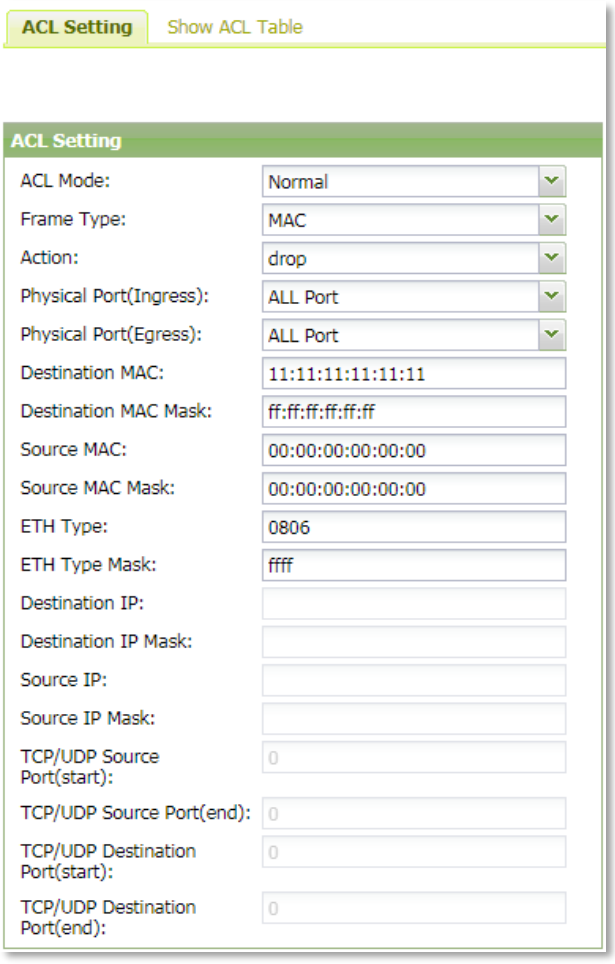


Figure 5-23 ACL Setting

Before clicking “Apply” to set the ACL setting, please make sure that the rules will not cause the WEB management to drop. After clicking the “Apply” button, users can check the rules in “**Show ACL Table**”.

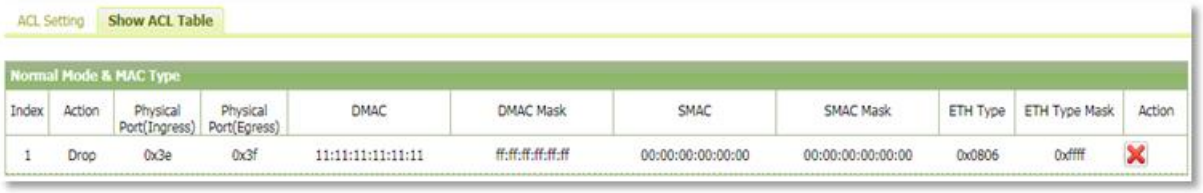


Figure 5-24 Show ACL Table

Table 5-1 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

16.12. User Interface

Users can enable or disable different network service ports in the ML630R Series. In the range of “Management IP/Mask”, the Telnet, SSH, HTTP, HTTPS and account protection are supported. The default setting of HTTPS is “**Permit**”.

- **Account Protection:** This is a way to temporary block brute-force attacks by simply locking out accounts for 5 minutes after 3 incorrect password attempts.
- **Management IP/Mask:** This field can fill in 172.16.5.0/16 as its format for example. If set the user interface to "Limited", only the operators set in the "Management IP/Mask" range have the right to control device.

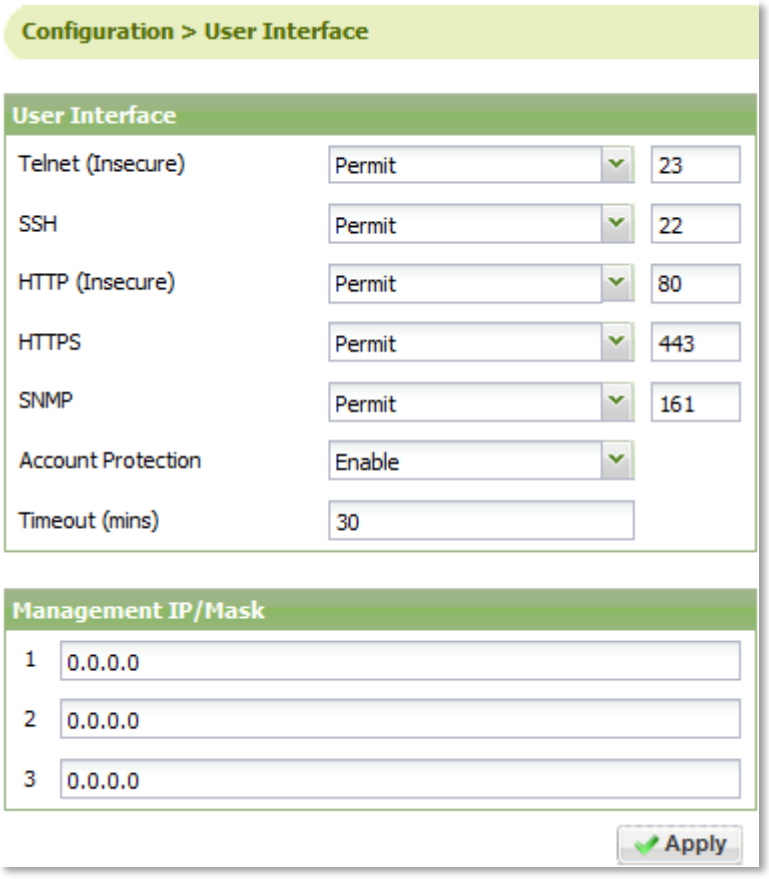


Figure 5-25 Local/Remote User Interface*

Note: Remote setting is only valid when ML630R is deployed as both the CO and CPE

16.13. Ser2Net

Repackaging RS-232 data as IP packets and then transmitting them through the network is one kind of smart solution for an industrial center. Not only can RS-232 data be transmitted through network, but also a remote device can be managed by the RS-232 interface.

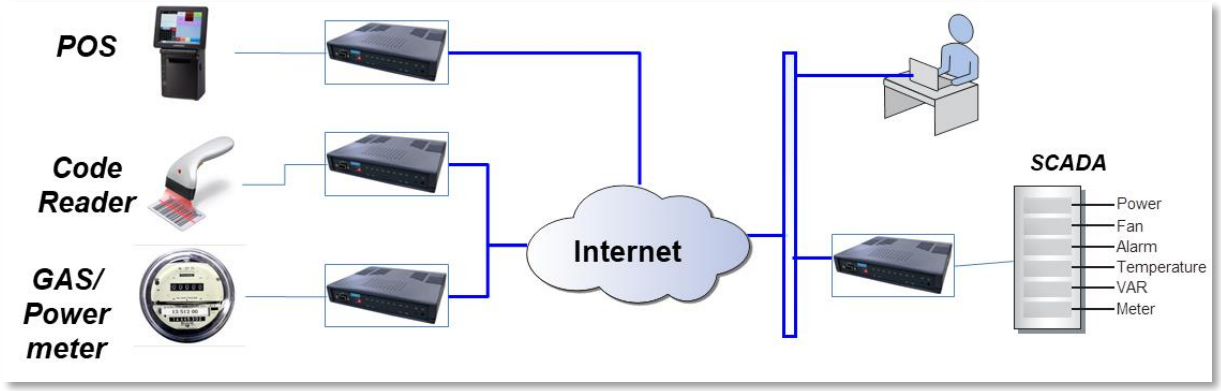


Figure 5-26 Serial port to IP application

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

> Caution:
>
> CAUTION
>
> When the **Admin** is turned to **ON,** the Ser2Net function may affect the console functionality. Please remember to use a static IP address for WEB management, in case either Console or Ser2Net is used.

- **Link Type** –Telnet, TCP and UDP mode can be selected. The Telnet and TCP type can choose Server or Client mode of the Serial port as a virtual console that connects with a remote device. 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 the timer is exceeded.
- **Baud Rate (bps)** – The serial port data speed. Can be configured as 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200bps.
- **Data Bit** – The data bit length in asynchronous frames for Serial transmission. 5, 6, 7 or 8 bits can be selected.
- **Parity Bit** – The type of parity check in asynchronous frames for Serial transmission. None, Even or Odd types can be selected.
- **Stop Bit –** The length of the stop bit in asynchronous frames for Serial transmission. One (1) or two (2) stop bits can be selected.

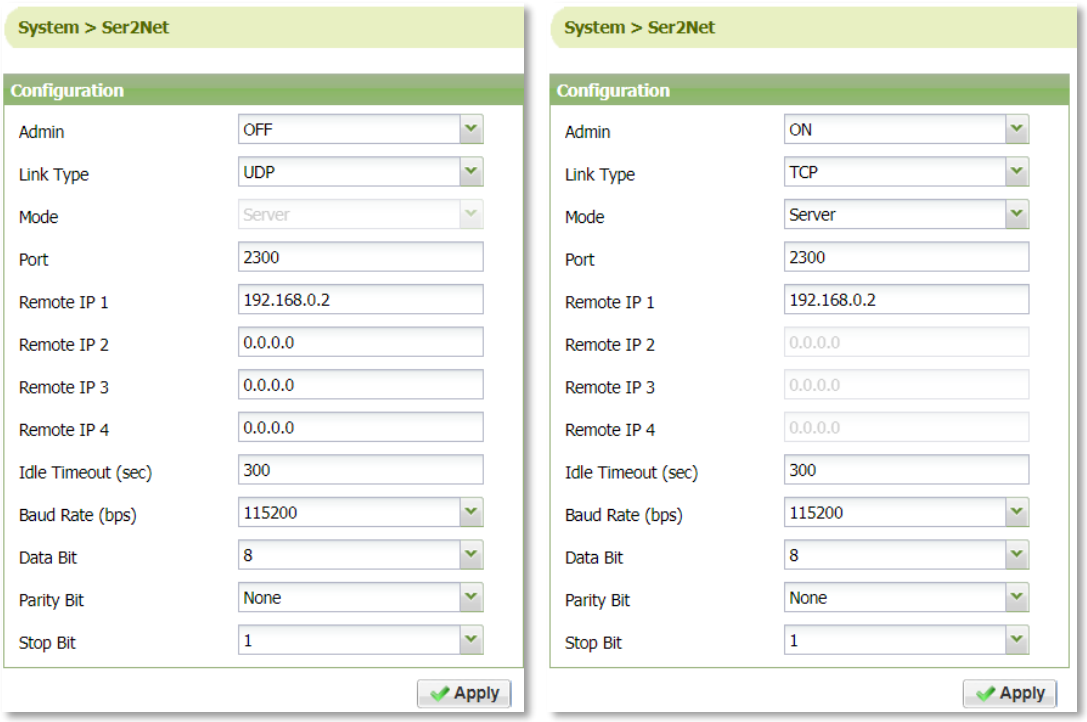


Figure 5-27 Convert serial port to IP Network

17. Bridge / Routing

17.1. General

There are two main windows in this menu, **"QoS Setup"** and **"Aging-Time"**. To quantitatively measure the quality of network service, several related aspects of the network service are often considered, such as packet loss, bit rate and transmission delay. The ML630R has the ability to 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 is 300 seconds; users can configure it for saturated release time.

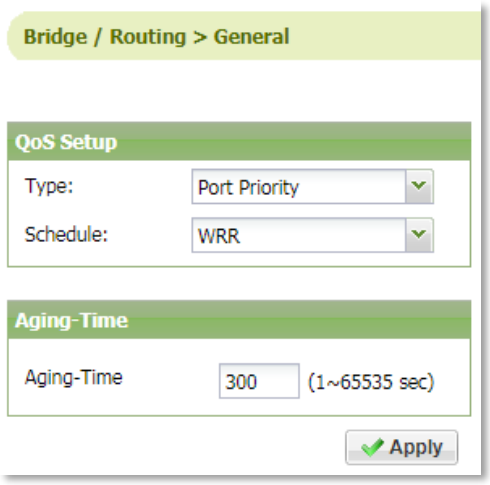


Figure 5-28 QoS Setup

17.2. VLAN

There are three VLAN rules available on the ML630R Series - "**Port-based**", "**Tag based**" and "**Q-in-Q**". The default parameter is "Port-based" for transmitting all traffic. For further management, switching the VLAN rule to "Tag-based" is the first step to enable basic VLAN and VLAN translation.

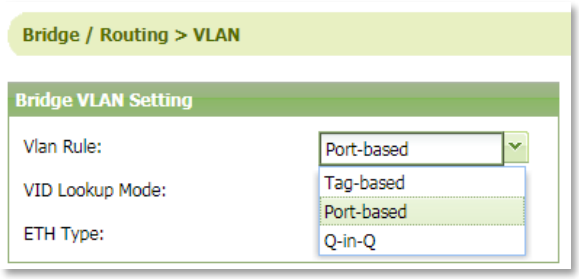


Figure 5-29 VLAN Rule

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

- Port-based VLAN

Port-based VLAN is a logical group of ports. This function is the default configuration and users will be unable to define the Ethernet switch when this option is chosen. Traffic within the VLAN will be forwarded to LAN 1-4. Therefore, users can use this setting to easily check VLAN traffic and connectivity.

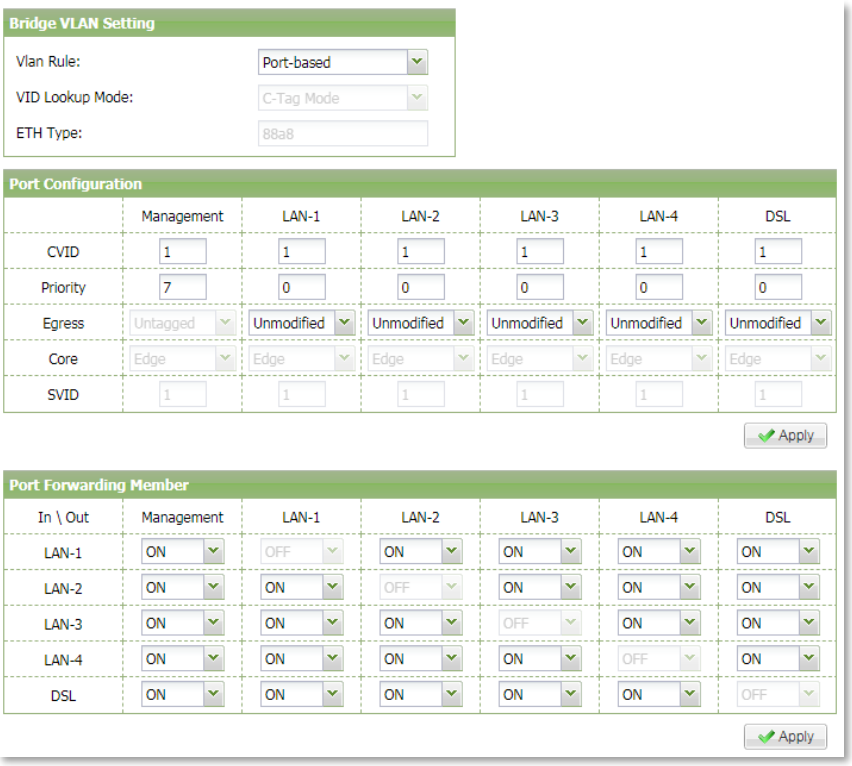


Figure 5-30 Port-based VLAN

- 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.

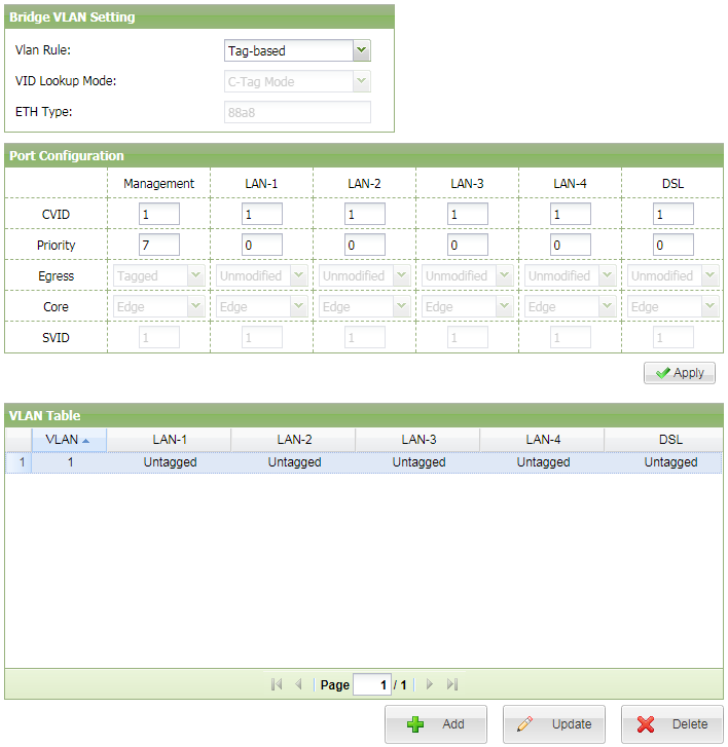


Figure 5-31 Tag-based VLAN

- 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 at the same frame. The main purpose is adding a VLAN tag to a VLAN-tagged packet that is defined by an external network without having to change the original packet.

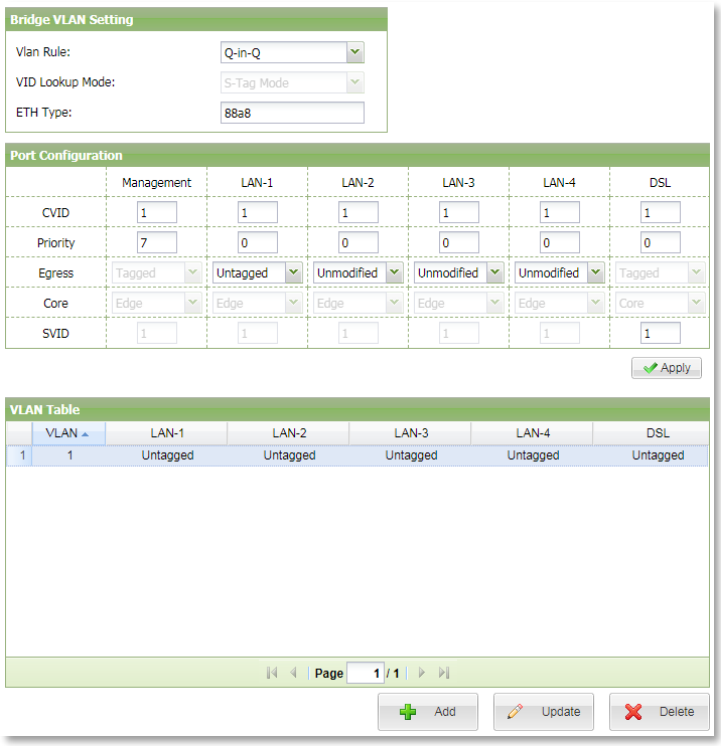


Figure 5-32 Q-in-Q

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

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

17.3. Virtual IP

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

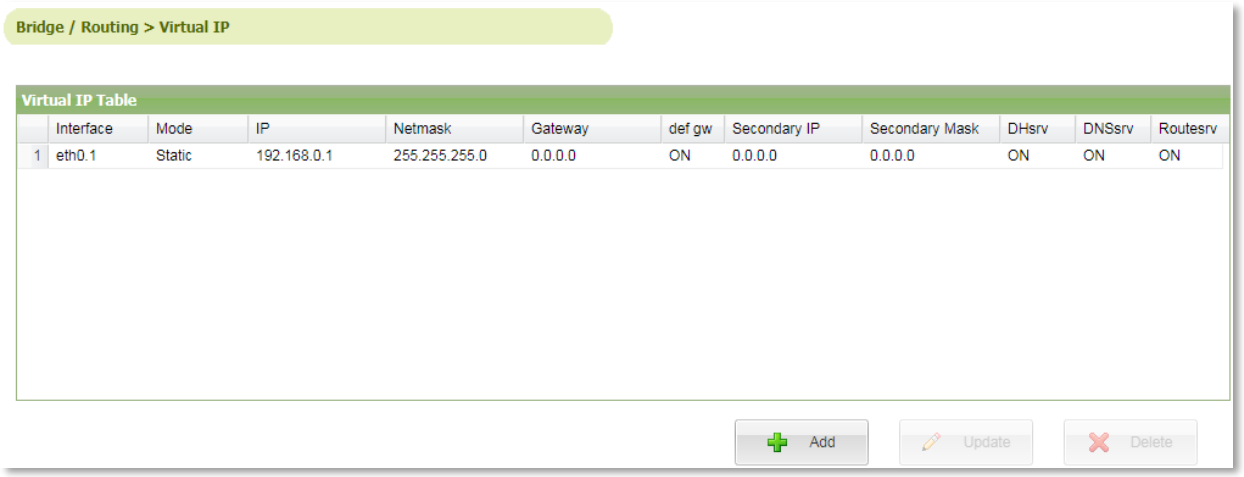


Figure 5-33 Virtual IP

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

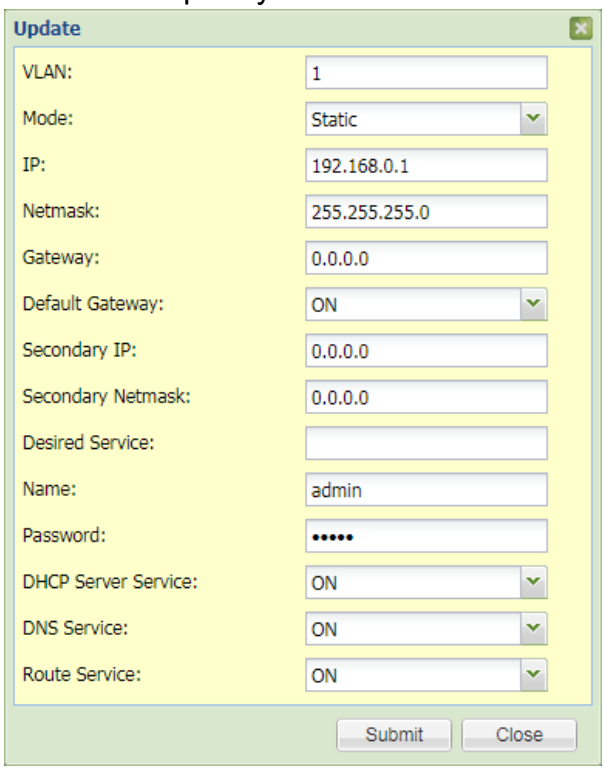


Figure 5-34 Edit Virtual IP

17.4. 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 tab is “**Routing Table**”, to check routing rules conveniently. The rules refer to IP, default gateway from the “**Virtual IP**” function. Users can check all rules before further configuring the routing application.

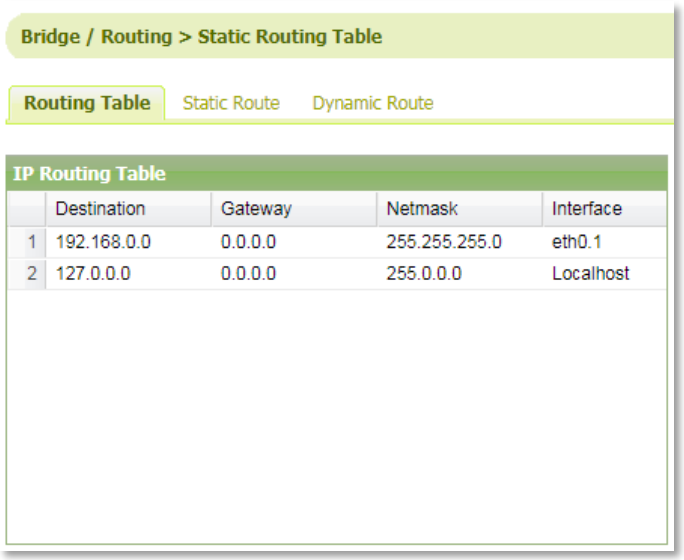


Figure 5-35 Routing Table

- **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 the operators’ requirements. If operators do not configure it, routing rules will refer to the “**Routing Table**”. When users start to configure rules in it, remember to configure “Interface” for output interface (eth0.1 or others).

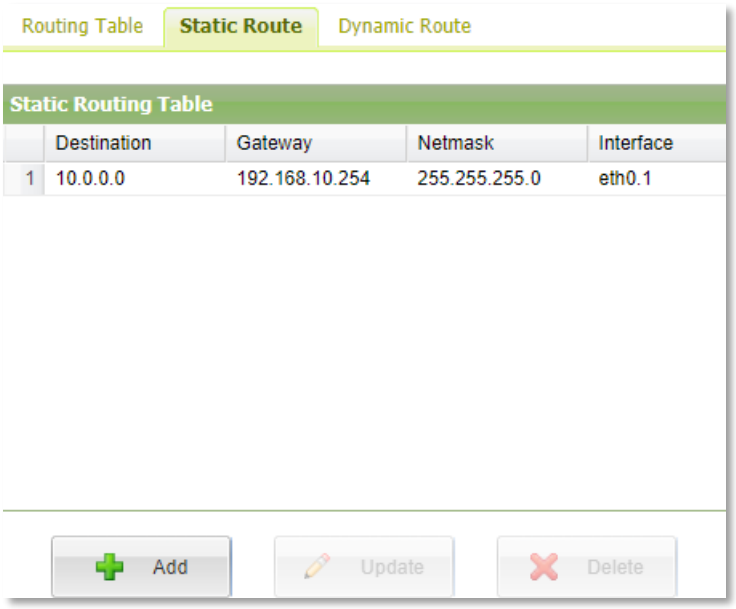


Figure 5-36 Static Route

- **Dynamic Route**: ML630R supports RIPv1(Classful Routing Protocol), RIPv2(Classless Routing Protocol), OSPFv2 and BGP4 routing protocols. 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).

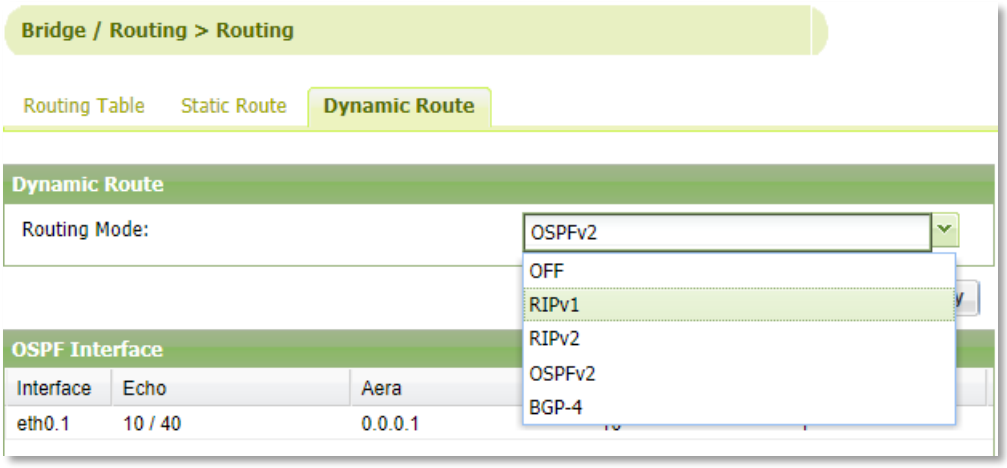


Figure 5-37 Dynamic Route

17.5. 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.

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.

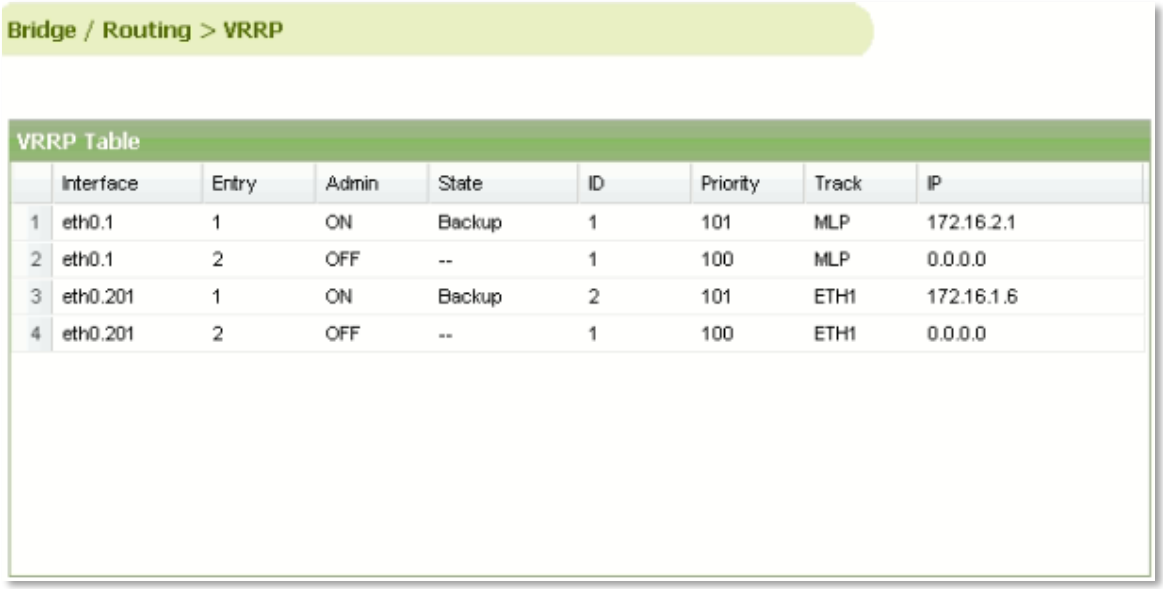


Figure 5-38 VRRP Table

17.5.1. VRRP Table

After the virtual IP has been configured on a 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 an additional virtual router to do load balance when needed.

In the example below, the virtual IP located at VLAN-1 (eth0.1) and VLAN-201 (eth0.201) is the example for the virtual WAN and LAN routers.

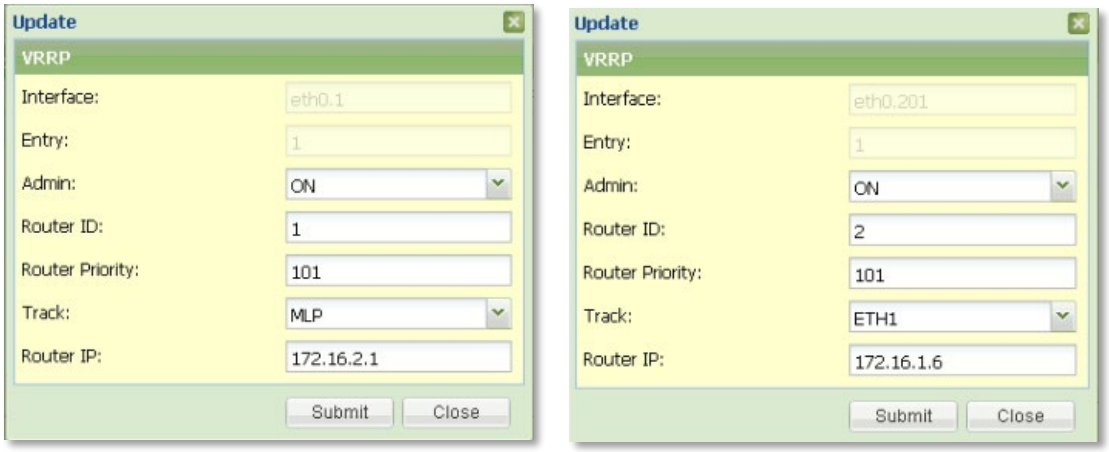


Figure 5-39 Setup VRRP Table

- **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.
- **Track**: Used to update the priority of the interface depending on whether it is up or down. The priority will decrease 20 when the interface is down. 101 will change to 91 for comparing with the opposite interface.
- **Router IP**: The virtual router IP address. It is the virtual router for each WAN and LAN routers.

17.6. NAT

Users have to enable "**Tag-based**" or "**Q-in-Q**" in VLAN rule to activate the routing mode, and then place VLANs in the VLAN table to configure "**NAT**". The default tab is "**NAT table**", with "**Configuration**" and "**Conntrack Table**" tabs also available.

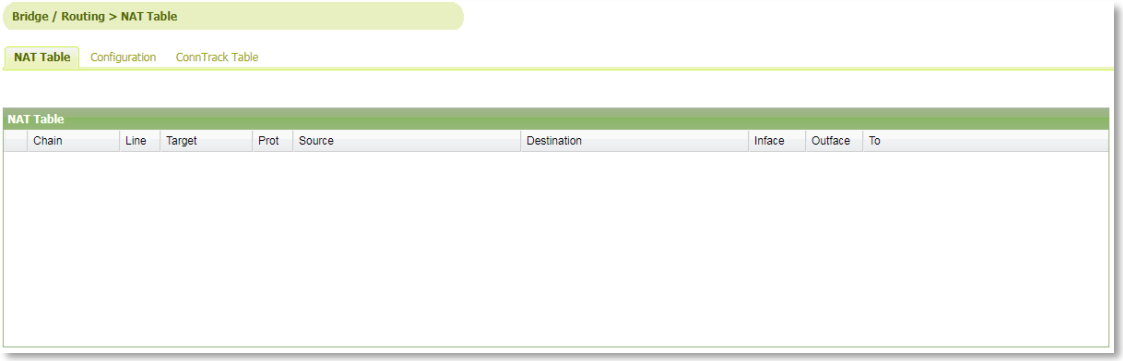


Figure 5-40 NAT Table

17.6.1. NAT Table

There are three options in the NAT table, "**Add**", "**Update**" and "**Delete**". If users would like to add a NAT rule, they can click the "**Add**" button, or update and delete any rules. For instance, clicking the "**Add**" button, the menu will display "**Source**", "**Destination**", "**Translation**" and "**To**" fields.

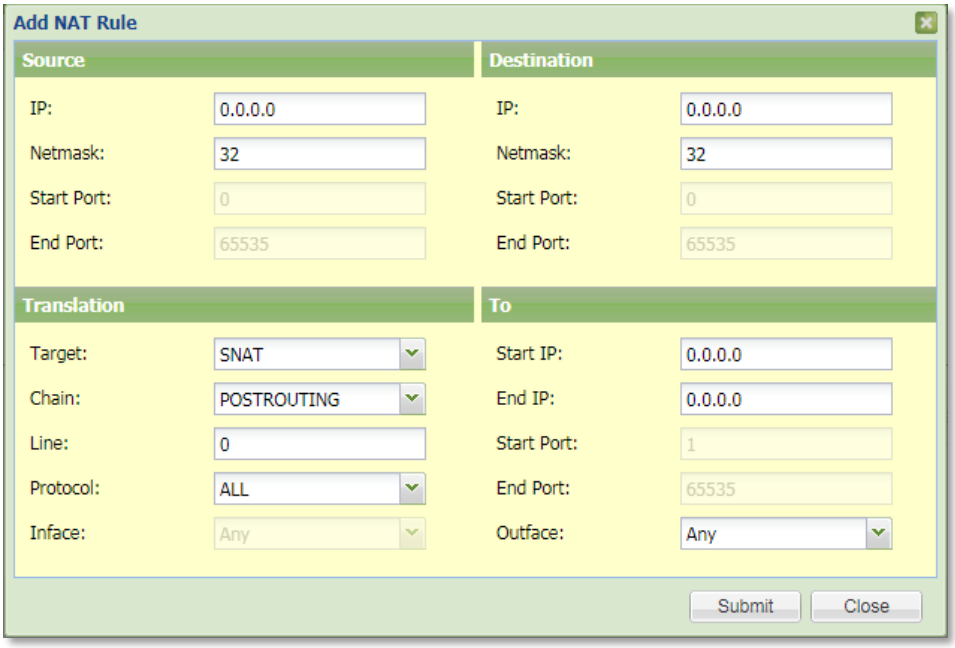


Figure 5-41 NAT Table

To start with, select "**Translation**" to configure **NAT**, **MASQUERADE** or **DNAT**. By 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 choosing the output interface for DNAT.

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

➢ **Protocol**: The default is "**ALL**". Other options are "**TCP**" and "**UDP"**. Only if the condition is "**TCP**" or "**UDP**" can the start and end port numbers be configured.

➢ **Inface**: Can be only configured by PREROUTING of DNAT mode and choosing the interface which refers to "**Virtual IP**".

- Source

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

➢ **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 only be configured if the protocol is not "**ALL**".

- Destination

- **IP**: A specified IP or a range of destination IPs.
- **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 only be configured if 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 the original IP. The initial IP in the range is "**Start IP**".
- **End IP**: The last IP in the range is "**End IP**".
- **Start Port** & **End Port**: Can only be configured if the protocol is not "**ALL**".
- **Outface**: Can be only configured by PREROUTING of DNAT mode and choosing the interface which refers to "**Virtual IP**".

17.6.2. 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

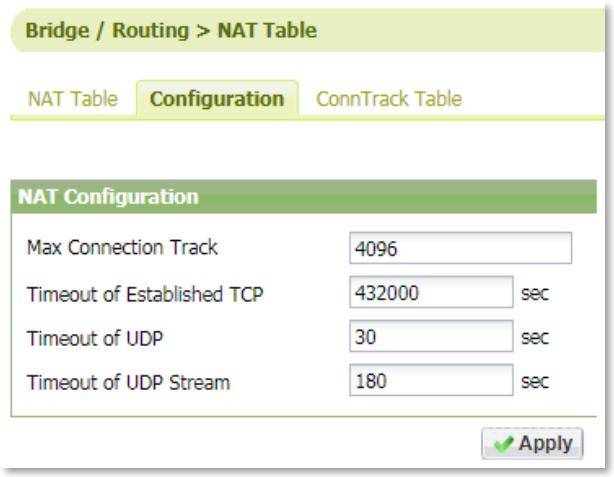
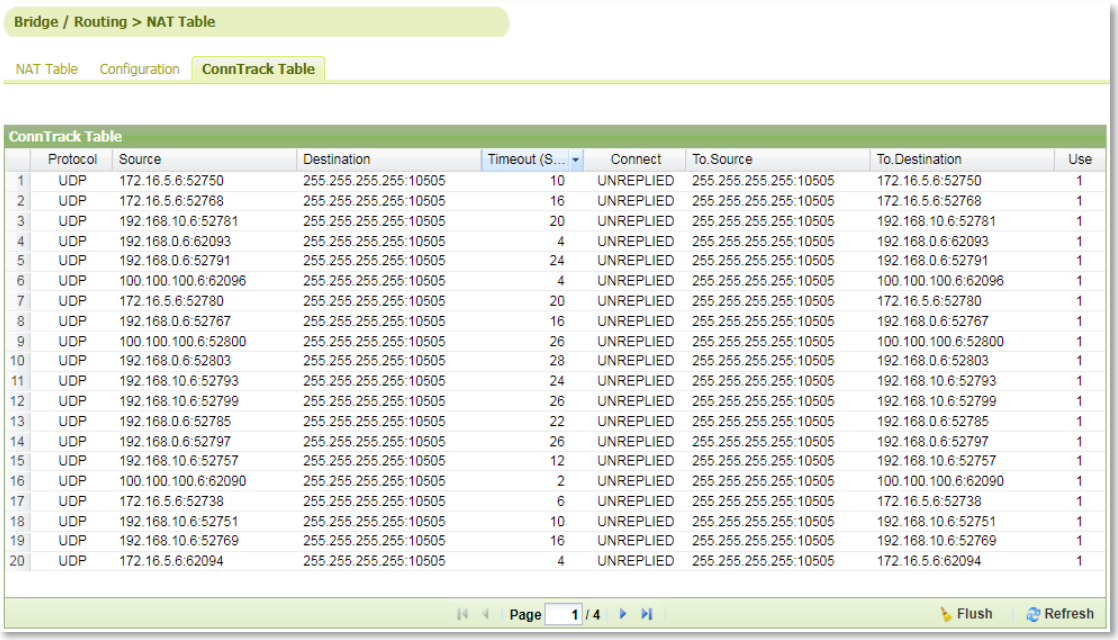


Figure 5-42 NAT Configuration

17.6.3. Conntrack Table

"Connection Tracking Table" is very important for a network manager for tracking and observing the status of data packages in the transmission network. Parameters include TCP/UDP, source and destination IP addresses, timeout and connection status.



	Protocol	Source	Destination	Timeout (S...	Connect	To.Source	To.Destination	Use
1	UDP	172.16.5.6:52750	255.255.255.255:10505	10	UNREPLIED	255.255.255.255:10505	172.16.5.6:52750	1
2	UDP	172.16.5.6:52768	255.255.255.255:10505	16	UNREPLIED	255.255.255.255:10505	172.16.5.6:52768	1
3	UDP	192.168.10.6:52781	255.255.255.255:10505	20	UNREPLIED	255.255.255.255:10505	192.168.10.6:52781	1
4	UDP	192.168.0.6:62093	255.255.255.255:10505	4	UNREPLIED	255.255.255.255:10505	192.168.0.6:62093	1
5	UDP	192.168.0.6:52791	255.255.255.255:10505	24	UNREPLIED	255.255.255.255:10505	192.168.0.6:52791	1
6	UDP	100.100.100.6:62096	255.255.255.255:10505	4	UNREPLIED	255.255.255.255:10505	100.100.100.6:62096	1
7	UDP	172.16.5.6:52780	255.255.255.255:10505	20	UNREPLIED	255.255.255.255:10505	172.16.5.6:52780	1
8	UDP	192.168.0.6:52767	255.255.255.255:10505	16	UNREPLIED	255.255.255.255:10505	192.168.0.6:52767	1
9	UDP	100.100.100.6:52800	255.255.255.255:10505	26	UNREPLIED	255.255.255.255:10505	100.100.100.6:52800	1
10	UDP	192.168.0.6:52803	255.255.255.255:10505	28	UNREPLIED	255.255.255.255:10505	192.168.0.6:52803	1
11	UDP	192.168.10.6:52793	255.255.255.255:10505	24	UNREPLIED	255.255.255.255:10505	192.168.10.6:52793	1
12	UDP	192.168.10.6:52799	255.255.255.255:10505	26	UNREPLIED	255.255.255.255:10505	192.168.10.6:52799	1
13	UDP	192.168.0.6:52785	255.255.255.255:10505	22	UNREPLIED	255.255.255.255:10505	192.168.0.6:52785	1
14	UDP	192.168.0.6:52797	255.255.255.255:10505	26	UNREPLIED	255.255.255.255:10505	192.168.0.6:52797	1
15	UDP	192.168.10.6:52757	255.255.255.255:10505	12	UNREPLIED	255.255.255.255:10505	192.168.10.6:52757	1
16	UDP	100.100.100.6:62090	255.255.255.255:10505	2	UNREPLIED	255.255.255.255:10505	100.100.100.6:62090	1
17	UDP	172.16.5.6:52738	255.255.255.255:10505	6	UNREPLIED	255.255.255.255:10505	172.16.5.6:52738	1
18	UDP	192.168.10.6:52751	255.255.255.255:10505	10	UNREPLIED	255.255.255.255:10505	192.168.10.6:52751	1
19	UDP	192.168.10.6:52769	255.255.255.255:10505	16	UNREPLIED	255.255.255.255:10505	192.168.10.6:52769	1
20	UDP	172.16.5.6:62094	255.255.255.255:10505	4	UNREPLIED	255.255.255.255:10505	172.16.5.6:62094	1

Figure 5-43 NAT Configuration

17.7. DNS

DNS is the name service of Internet addresses that translates friendly domain names to numeric IP addresses. ML630R supports DNS Server & DNS cache. Firstly, users have to enable "**Tag-based**" in VLAN rule to activate the DNS function. If the modem acts as a DNS Server, enable the "**Authoritative Server Mode**". If users want to follow external 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)**: Is the time interval of transmitting DNS packages.
  - **Upstream Server-1**: Default IP is "**8.8.8.8**" referring to the external DNS server-1.
  - **Upstream Server-2**: Default IP is "**8.8.4.4**" referring to the external DNS server-2
  - **Authoritative Server Mode**: "**ON**" (Specified DNS Server), "**OFF**" (Random bypass)
- Authoritative Server Zone

  Users are able to "**Add**", "**Update**" and "**Delete**" specified DNS server rules. Below is 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

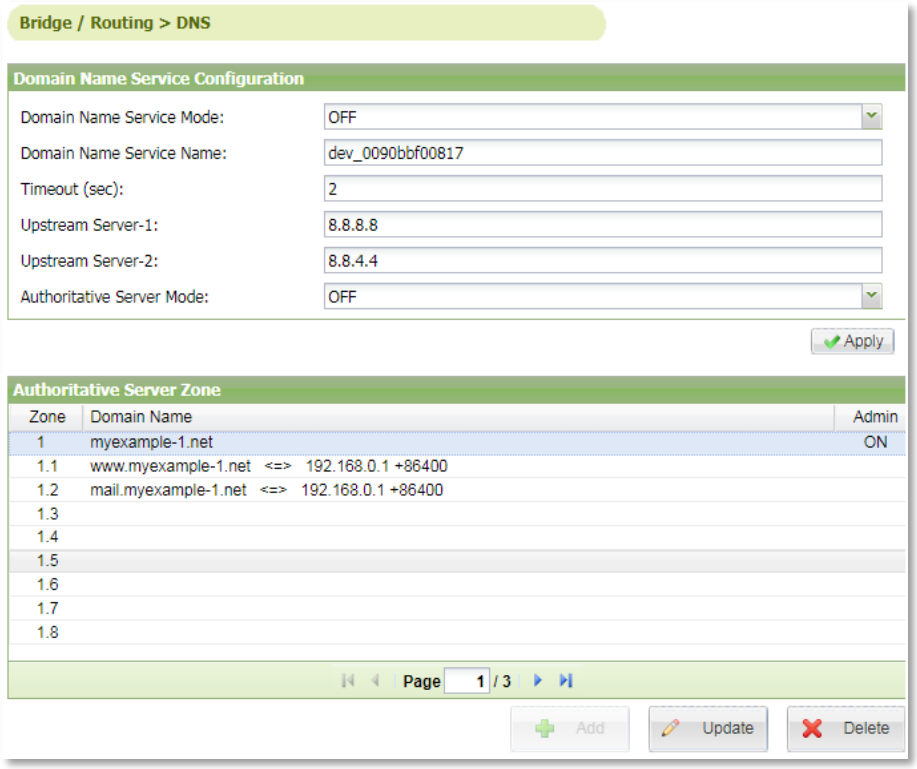


Figure 5-44 DNS Server/Cache

17.8. G.8032

ML630R provides ERPS (Ethernet Ring Protection Switch) according to ITU-T G.8032 standard. With this feature, not only a serial linear network can be supported but also ring topology. The downside of a serial linear network is any failure of any nodes or ports would affect traffic for the whole network. A ring network can resolve this issue because it is a redundant system. Ring protection can be established in ETH ports or DSL trunk.

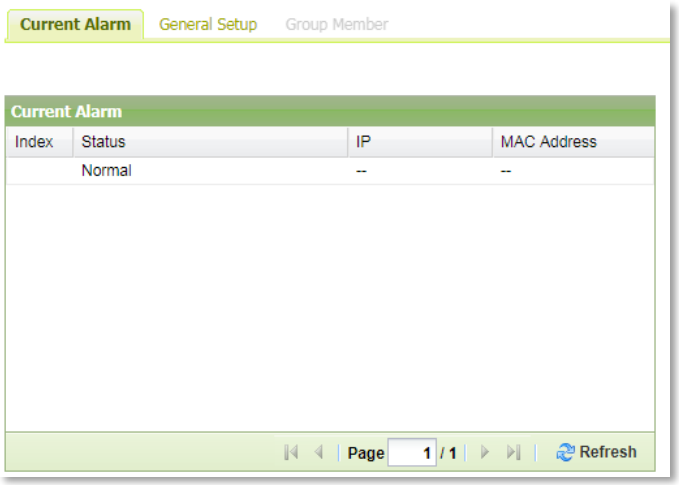


Figure 5-45 Current Alarm

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 the 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 the central unit with more capabilities that can decide whether others can join 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 a ring network, each unit needs at least two physical lines to connect to two other units. Choose LAN-1 to LAN-4 when using an Ethernet ring network.
- **Link-1**: Refer to the description of Link-0.
- **Ring Protection Link**: Select one data trunk to be the ring protection (to avoid loop errors). The chosen link will initially be shut down. If other trunks in this network fail, the mechanism will automatically enable the Ring Protection Link to recover the whole transmission. **Note**: Remember to configure the parameter at both ends of the ML630R.
- **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 are repeated.

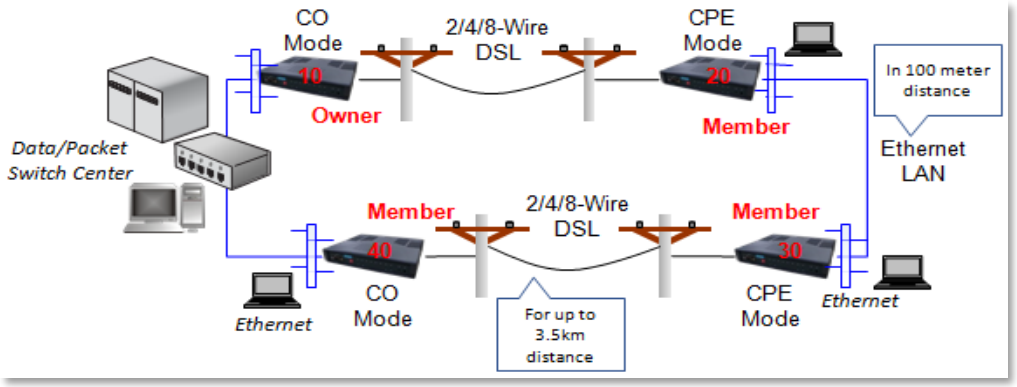


Figure 5-46 Owner and Member for Ring topology

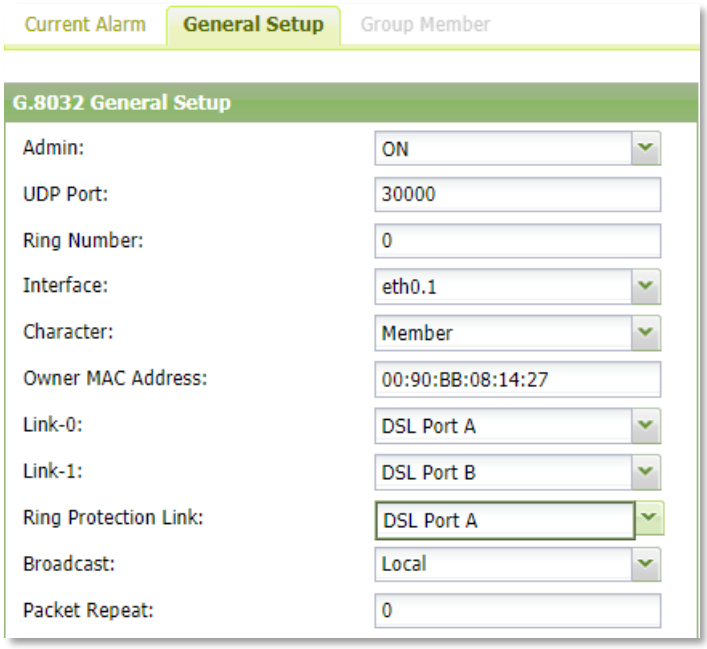


Figure 5-47 General Setup

- Group Member

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

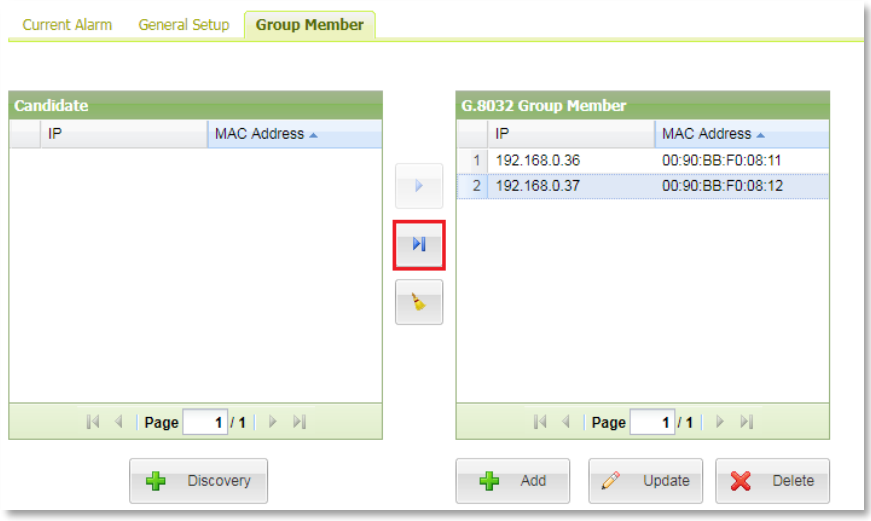


Figure 5-48 Group Member

17.9. RSTP

ML630R provides RSTP (Rapid Spanning Ring Protection) according to the IEEE 802.1w standard. With this feature, each device can be connected in a linear, ring or mesh topology and prevent traffic broadcast storms (Ethernet loops) in the network.

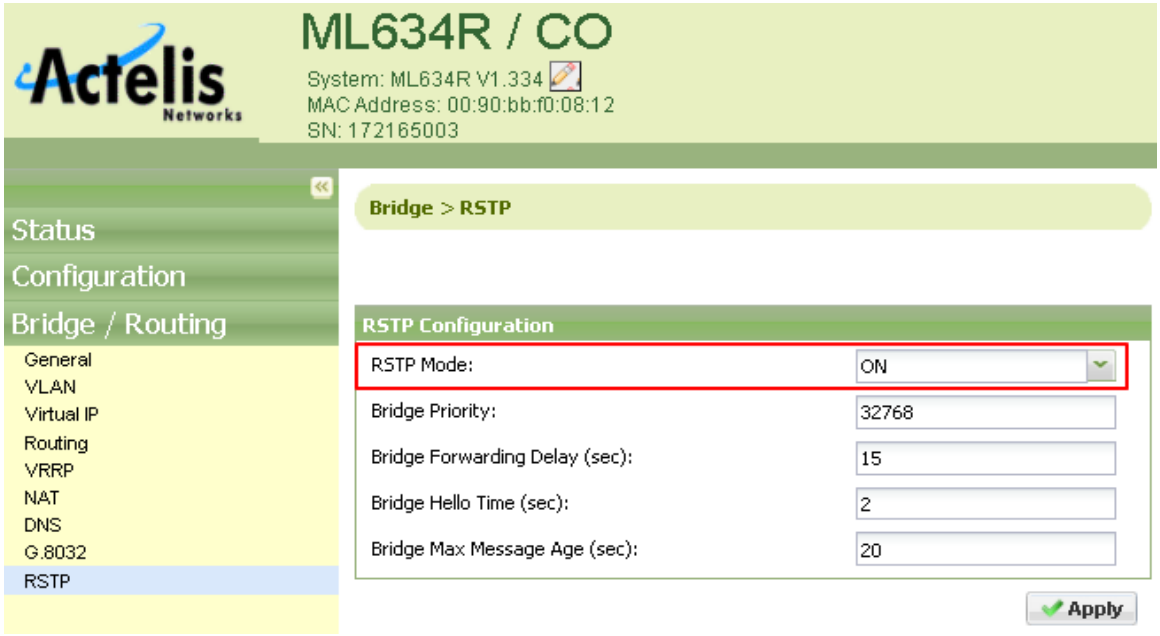


Figure 5-49 Rapid Spanning Tree Protocol (RSTP)

RSTP uses 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), to allow 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) is a field inside a BPDU packet and is eight bytes long. The first two bytes are the bridge priority, an unsigned integer of 0-65535. 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 is 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:** The message age is a mechanism to avoid RSTP loops. 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.

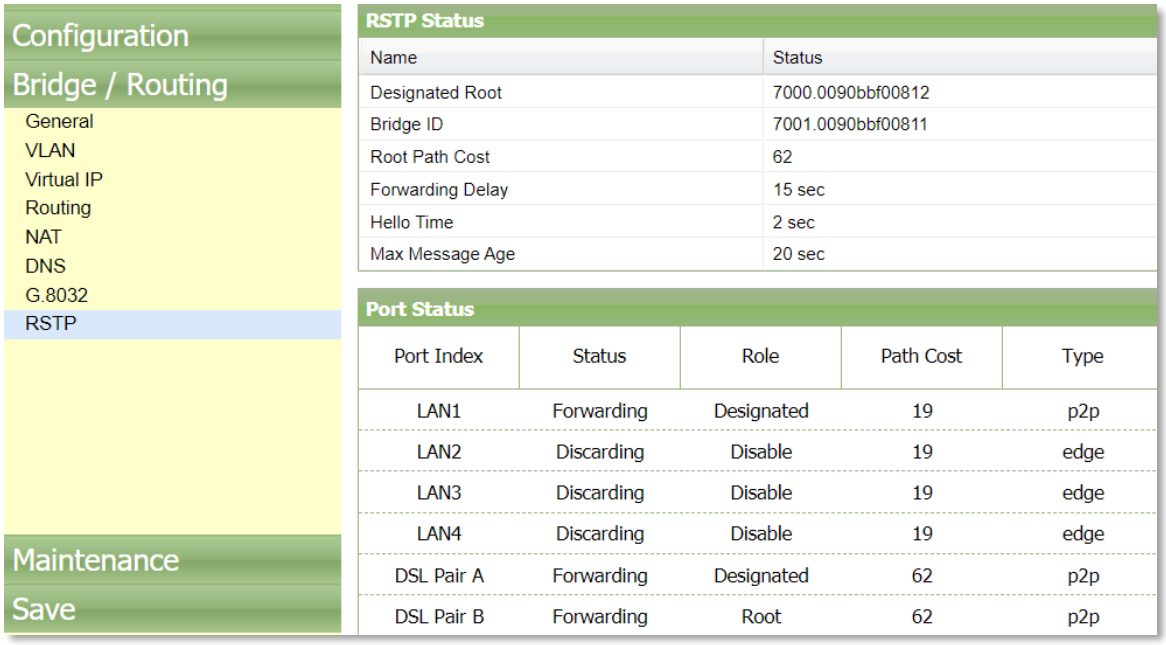


Figure 5-50 RSTP Status and Port Status

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

Table 5-2 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 for a short period of time while the Alternate Port and Backup Port replaces the Root port.
- **Discarding:** The Disable, Blocking and Listening port state in STP is the same as the Discarding port state in RSTP.

- Port Role

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

- 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:** A half-duplex port is considered as a shared port by default

18. Maintenance

18.1. Alarm Log

The alarm history is displayed in this section. The network manager can check different the severity levels of logs according to the system time.

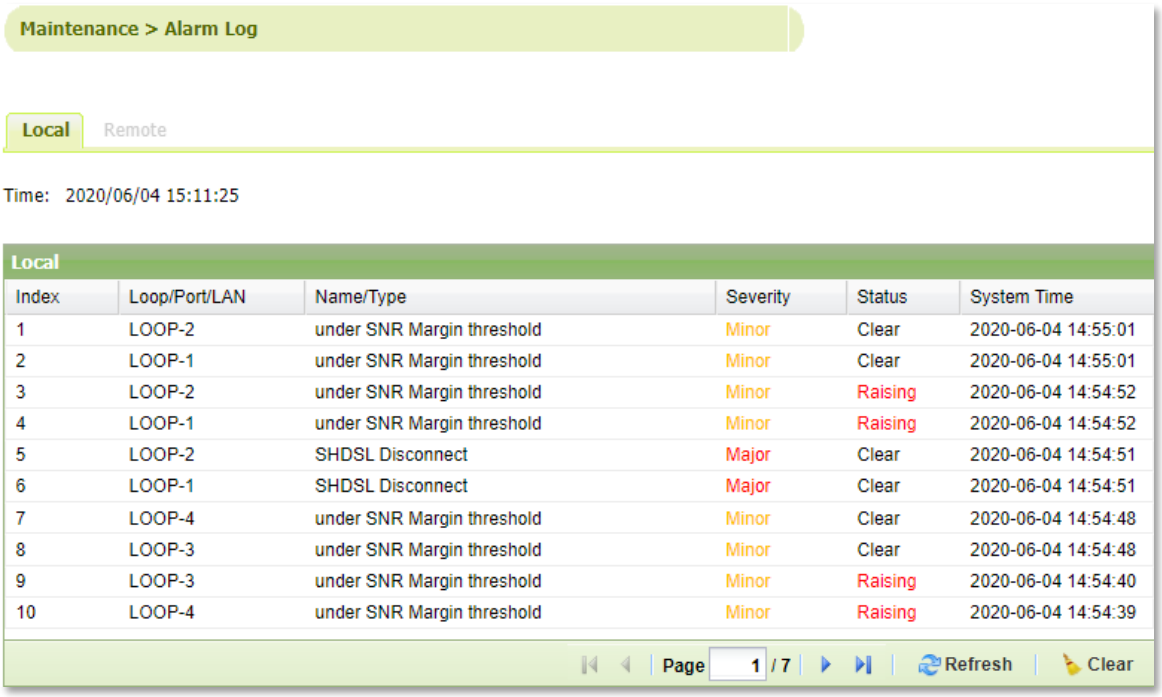


Figure 5-51 Alarm Log

18.2. Local Access Log

All IP accessed and WEB action logs are displayed in this section. The network manager can check all operation records together with the time that the actions were performed.

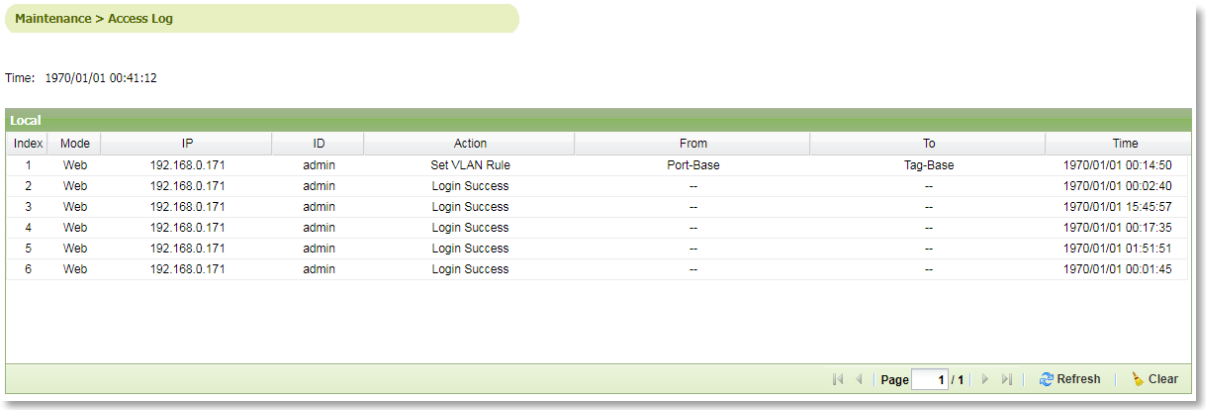


Figure 5-52 Access Log

18.3. 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 by simply locking out accounts for 5 minutes after 3 incorrect password attempts. The system displays any unauthorized IPs. When incorrect login authentication is entered more than five times, the ML630R will refuse the IP address. Manually clearing the table records will recover the blocked IPs.

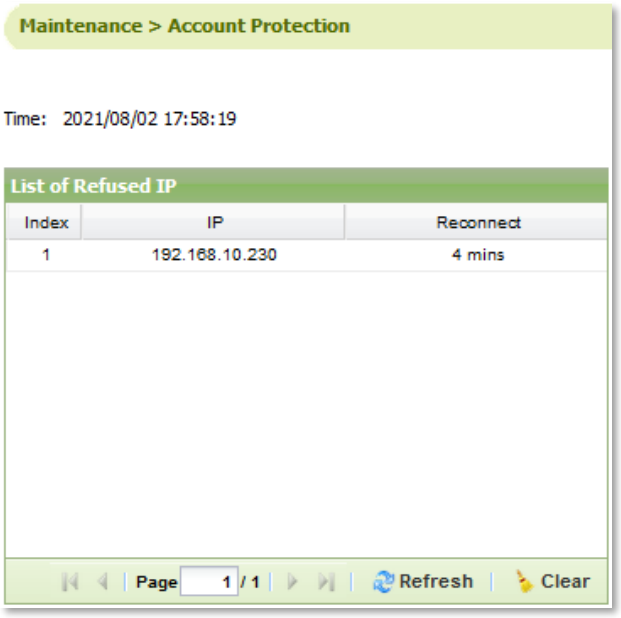


Figure 5-53 Account Protection

18.4. Performance History

The performance history shows the errors occurring on each loop by 15 minutes or 1 day duration. The system supports Local/Remote* G.SHDSL performance history. Users can manually update all records.

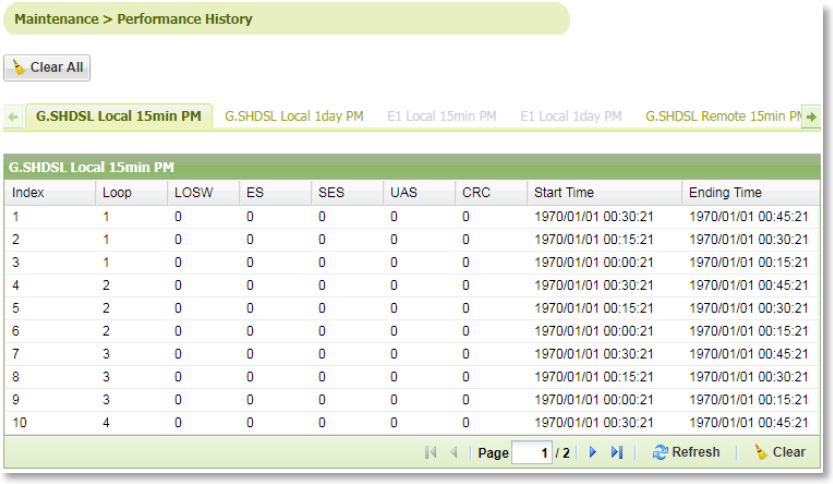


Figure 5-54 Performance History

18.5. 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.

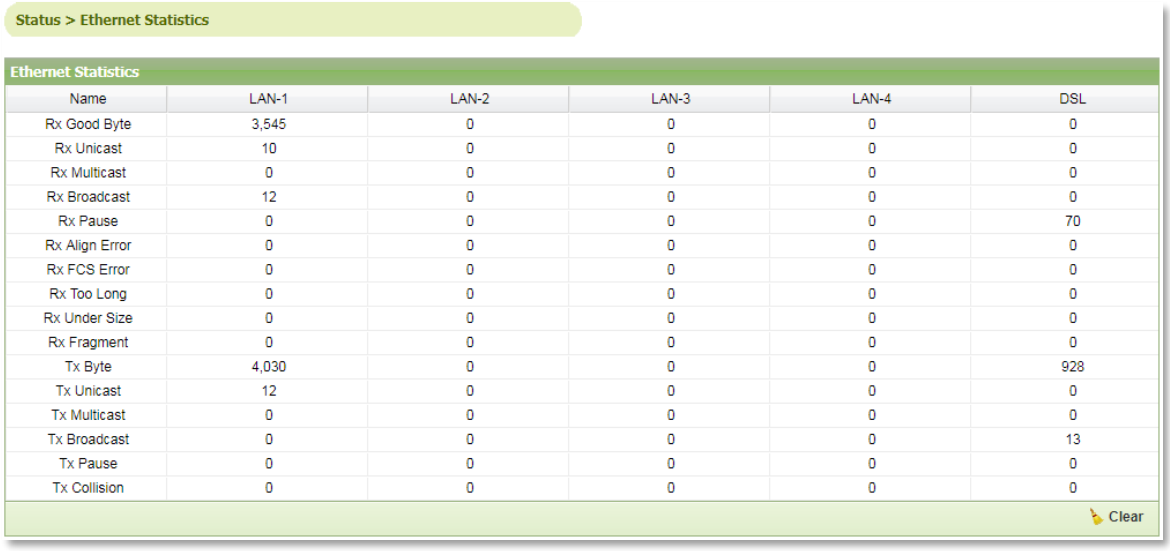


Figure 5-55 Ethernet Statistics

18.6. Software Default

This function is used to restore all settings to factory defaults except the device IP and management authority.

After clicking the “Apply” button, the pop-up window will show a confirmation message.

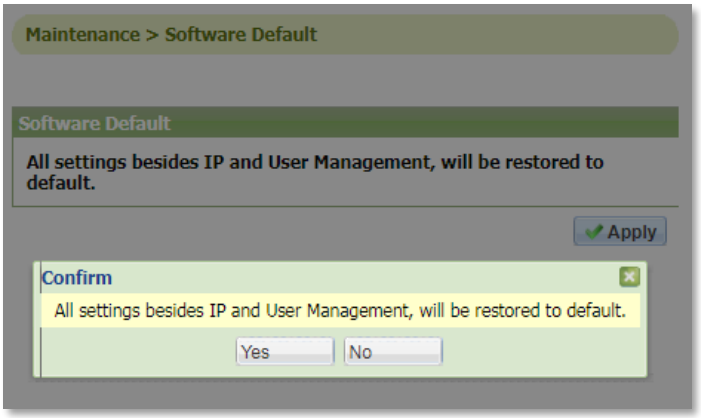


Figure 5-56 Software Default

18.7. Factory Default

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

After clicking the “Apply” button, the pop-up window will show a message to reconfirm.

Step 1: Click “Choose File” to open the folder and enter the software version file.

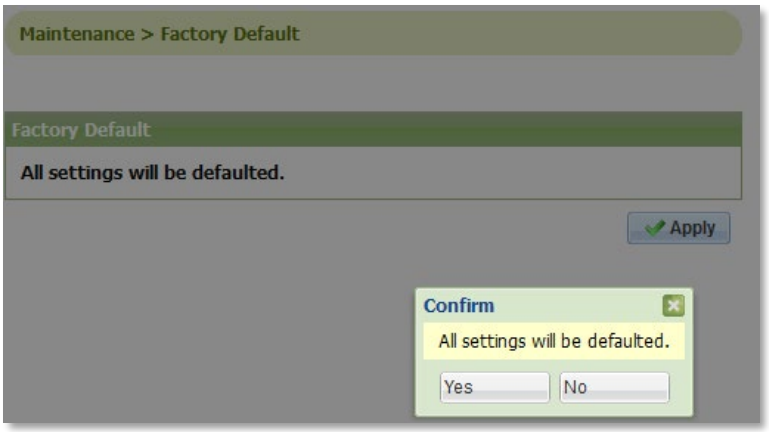


Figure 5-57 Factory Default

18.8. Software Upgrade

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

Step 1: Click “Choose File” to open the folder and enter the software version file.

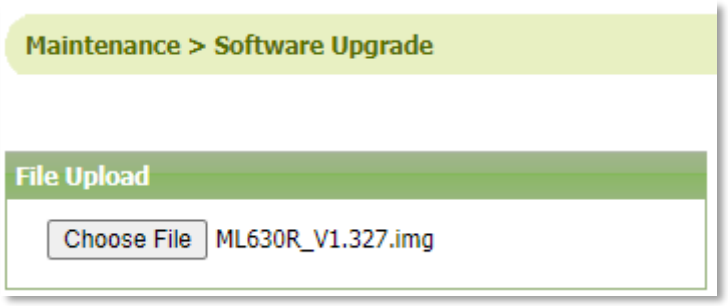


Figure 5-58 HTTP File Upload

Step 2: Select “**OK**” to save all current configurations

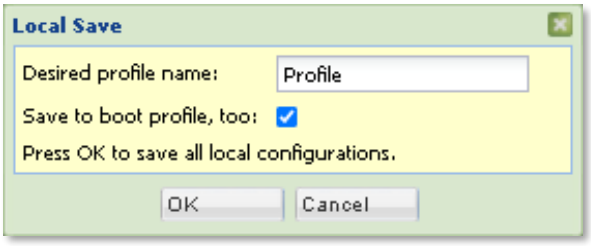


Figure 5-59 Local Save

Step 3: The system will start to upload the new software code

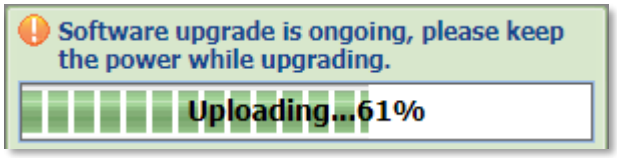


Figure 5-60 HTTP Uploading File

Step 4: Select “Yes” to upgrade the version. The process will start automatically after 20 seconds if no user response is entered.

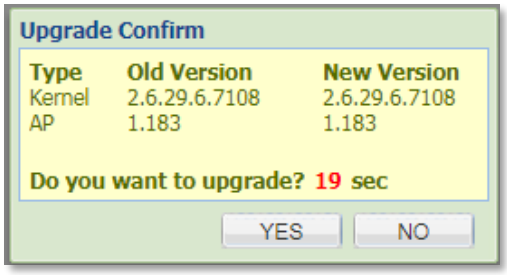


Figure 5-61 HTTP Upgrade Version Confirmation

Step 5: During upgrade procedure, all LEDs on the ML630R's front panel will blink at the same time. Do not turn off the power during this process. The total procedure takes about 3 minutes to return to standby mode.

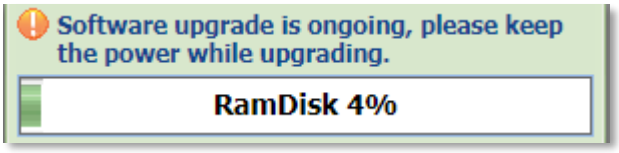


Figure 5-62 Upgrade Proceeding

18.9. SSL Setting

SSL supports a secure method for accessing the ML630R. By using HTTPs to access the WEB the ML630Rs are better protected from hacking attempts. To improve the security level of the modem, three types of SSL certification are supported.

SSLCaCertificateFile(.crt)

SSLCertificateFile(.crt)

SSLCertificateKeyFile(.key.pem)

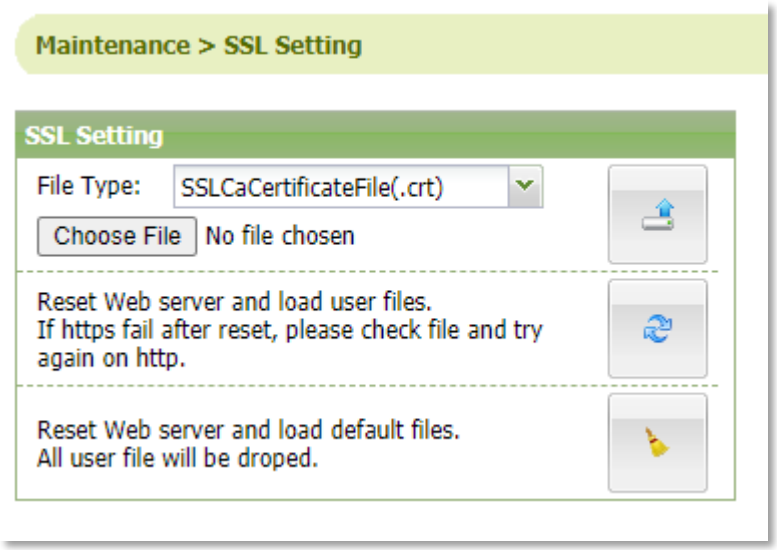


Figure 5-63 SSL Setting

18.10. Ping

This feature is used to verify whether the packet transmission path is reachable or is alive. Users may select “**Interface**” for path and input an IP address in “**Ping IP**” to test.

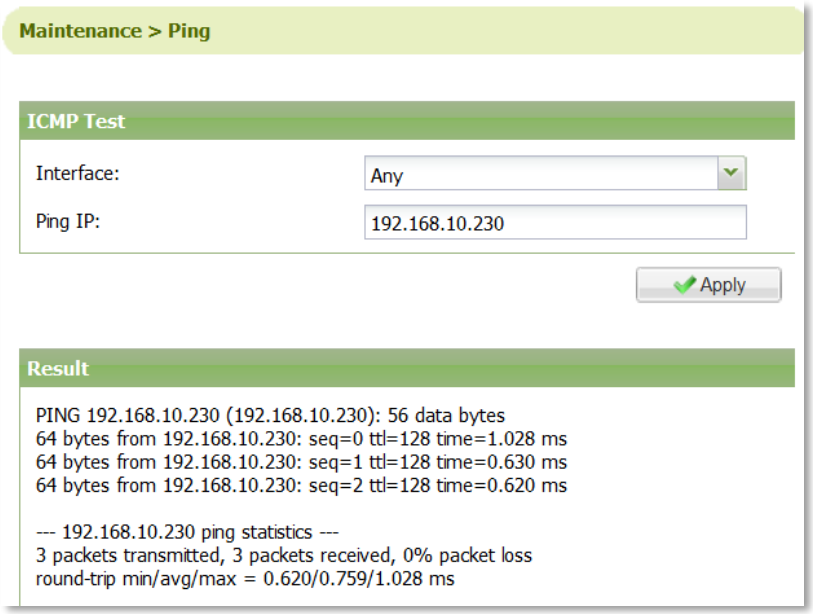


Figure 5-64 Ping

19. Save

19.1. Local Save

Save all Local configurations as a user profile. This will allow the ML630R to save the current configuration and restore it at the next power on.

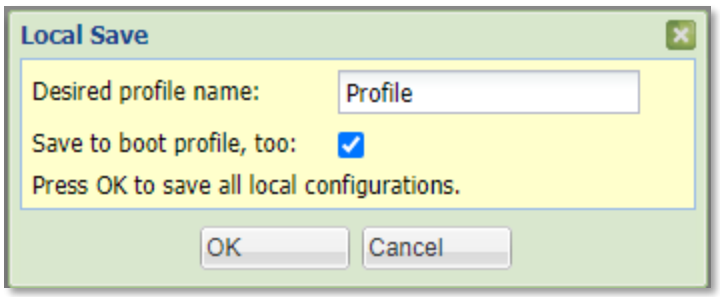


Figure 5-65 Local Save

20. About

20.1. Software Version

The system will show the correct model type and software version of ML630R series on local and remote modems.

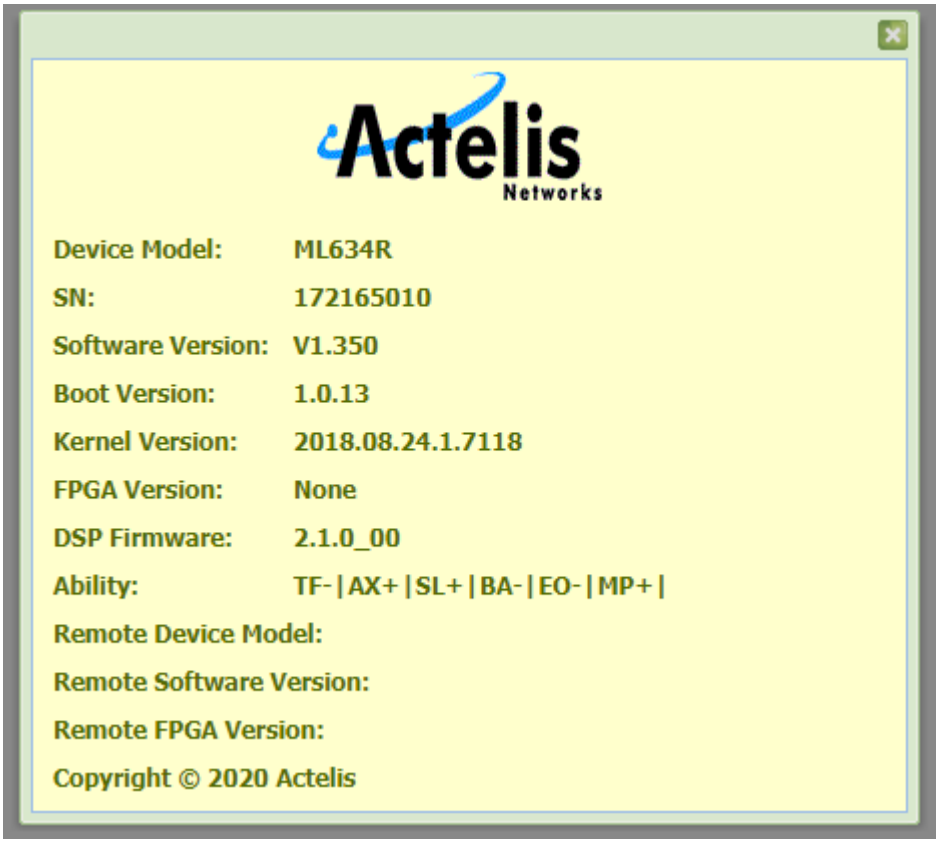


Figure 5-66 Local / Remote Software Version

21. Action

Figure 5-67 Action

- **Logout**: Return to the login page
- **Local System Reboot**: Restart the local modem.
- **Summary**: The operator can upload a summary file including all the configuration, modem status, alarm log, and Ethernet statistics to local storage. It can be analyzed by the network manager for further assistance.

22. Application Examples

22.1. Bridge ATM Application

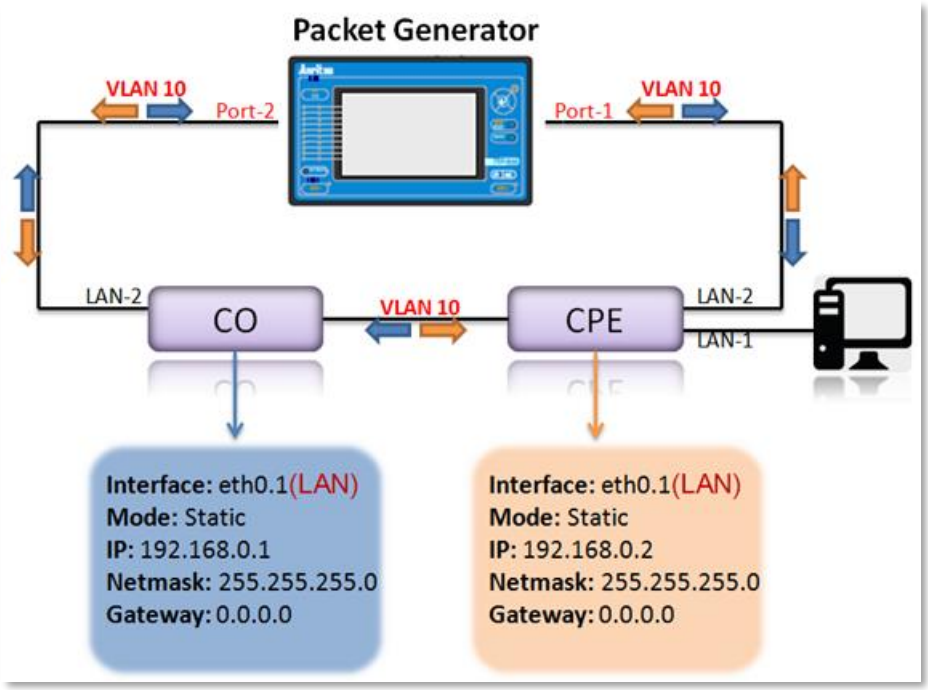


Figure 5-68 Bridge ATM Application

- < CO configuration >

1. Configuration > Local Setting > G.SHDSL

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

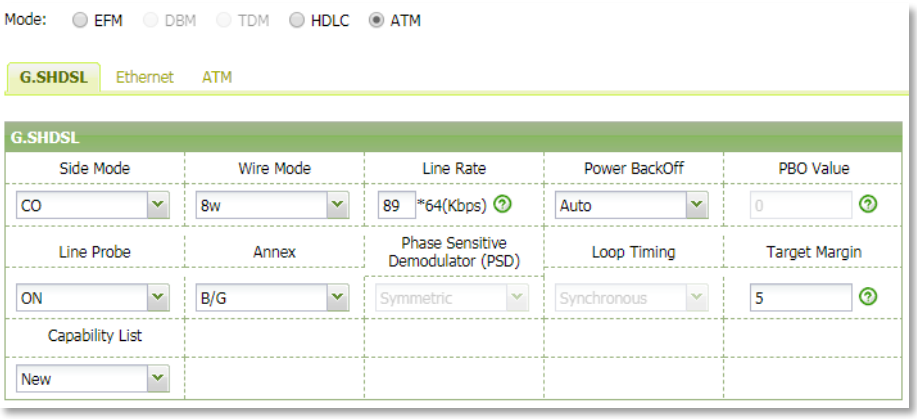


Figure 5-69 CO-G.SHDSL

2. Configuration > Local Setting > ATM

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

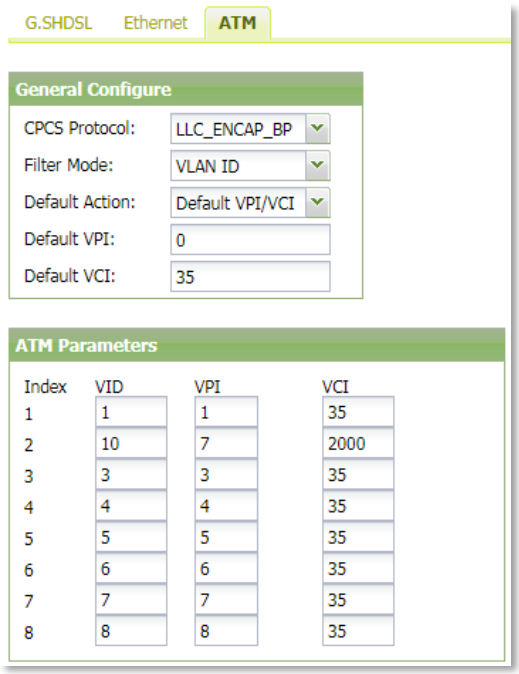


Figure 5-70 CO-ATM

3. Bridge / Routing > VLAN

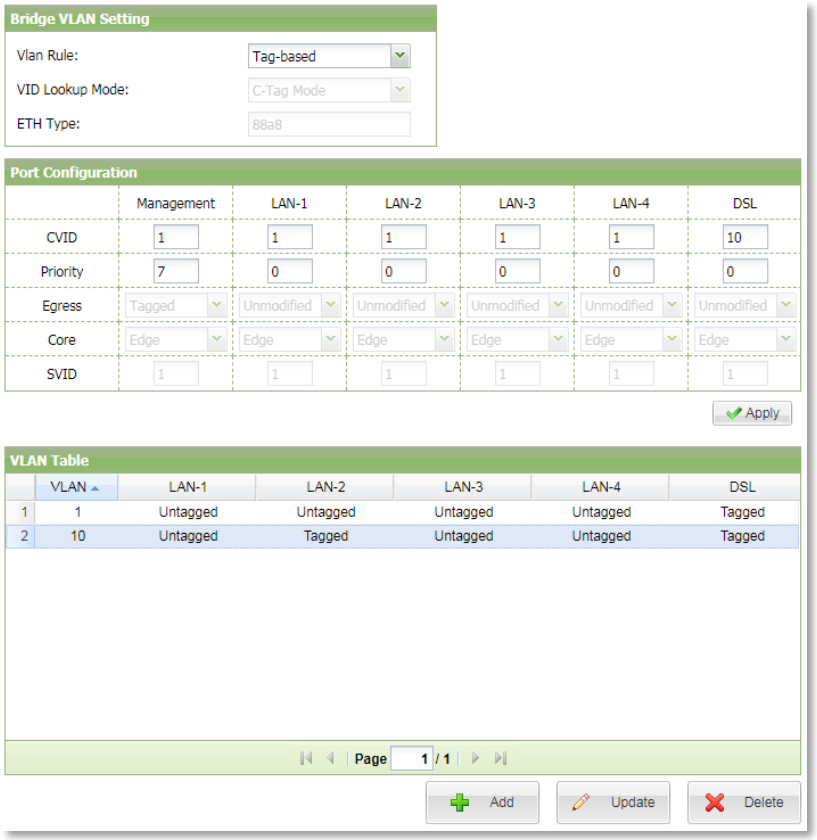


Figure 5-71 CO-VLAN

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

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

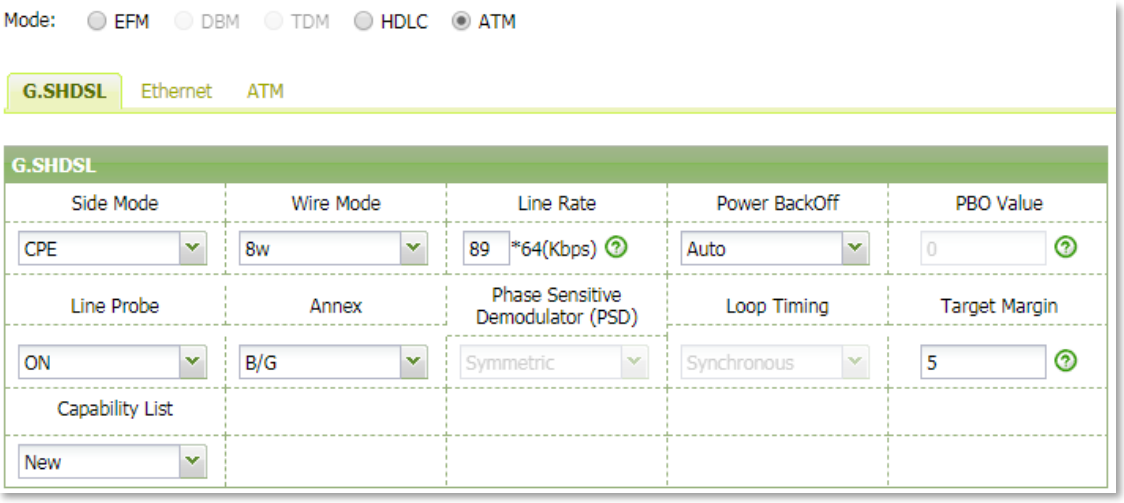


Figure 5-72 CPE-VLAN

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 5-73 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 connected, it will take about 10 ~ 30 seconds for the high-speed link to synchronize and for data to pass through the DSL. Do not forget to save the configuration.

22.2. VLAN Application

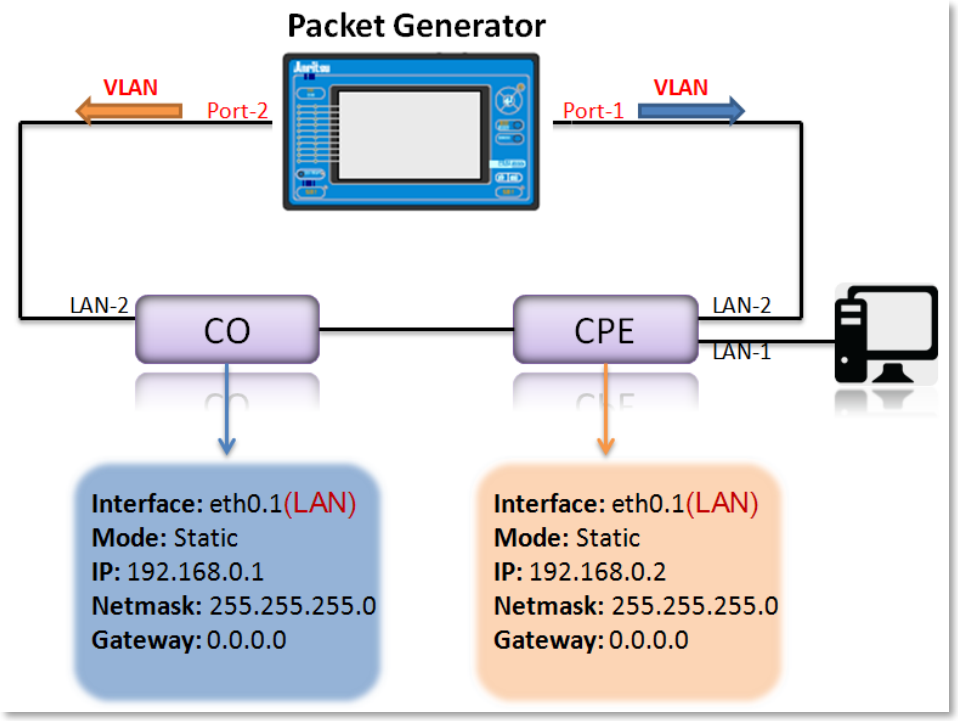


Figure 5-74 VLAN Application

- < CO configuration >

Configuration > Local Setting > G.SHDSL

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

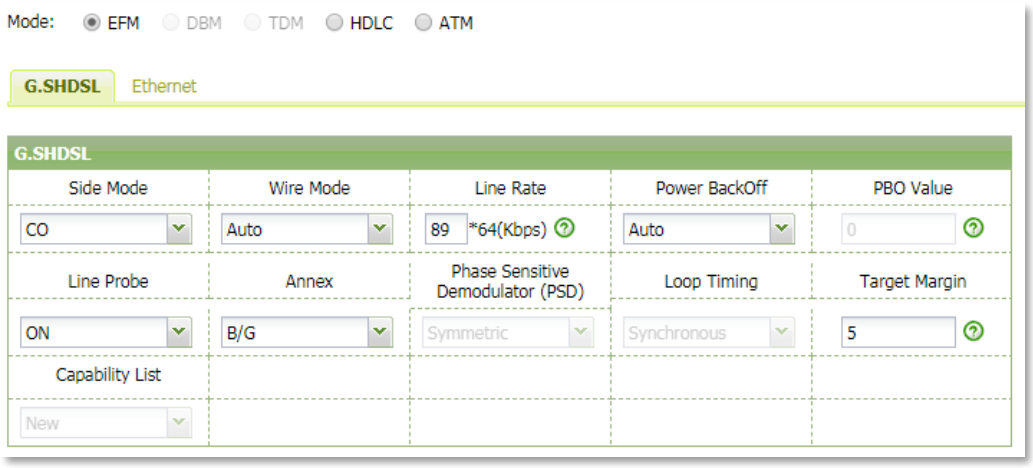


Figure 5-75 CO-G.SHDSL

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

The default master-slave relationship of ML634R is "**CPE**".

2. Configuration > General Setup > Local

Figure 5-76 CPE-General Setup

3. Bridge / Routing > VLAN

VLAN Rule= **Tag-based**

- Tag-based mode is defined as CVID (Egress), for comparing with the VLAN table.
- Add the VLAN in the table and configure different VLAN functions on each port. Below is an example.

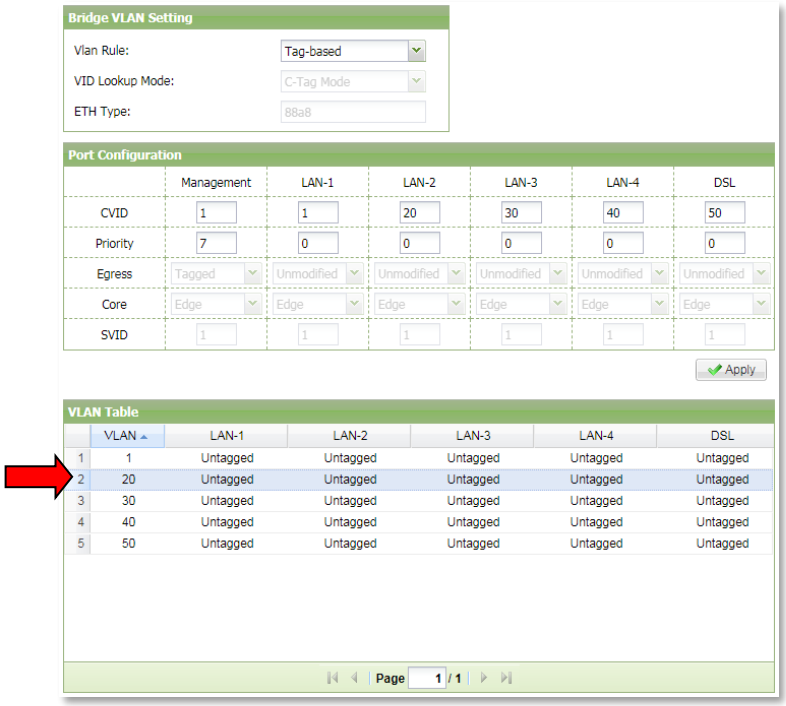


Figure 5-77 CPE-VLAN

** Note: Remember to save after configuring.

Test Result:

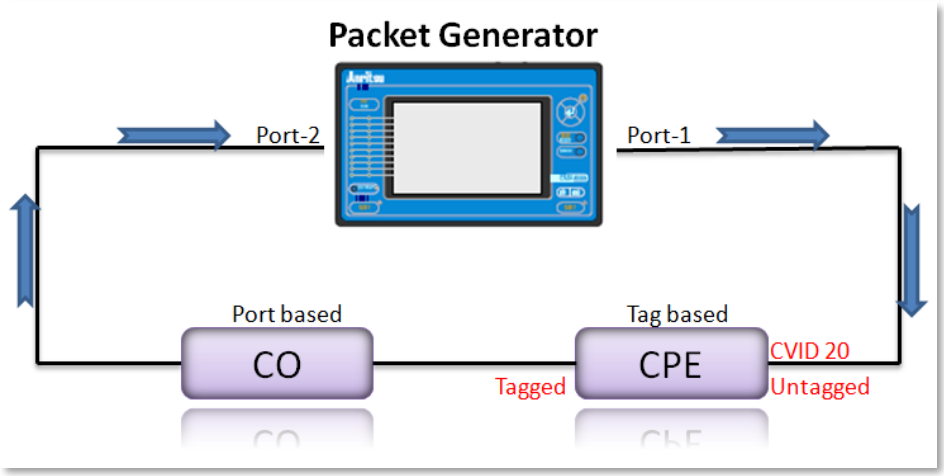


Figure 5-78 VLAN Test Result - 1

Table 5-3 VLAN Test Result – 1

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

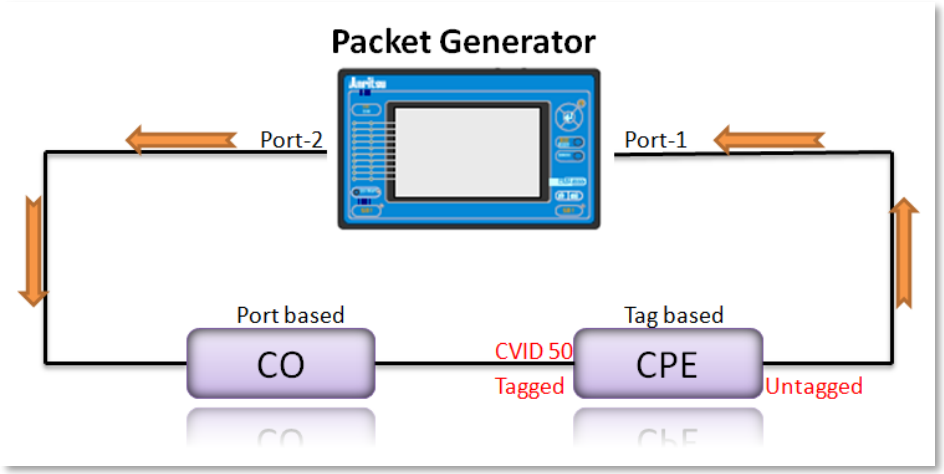


Figure 5-79 VLAN Test Result – 2

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

Table 5-4 VLAN Test Result – 2

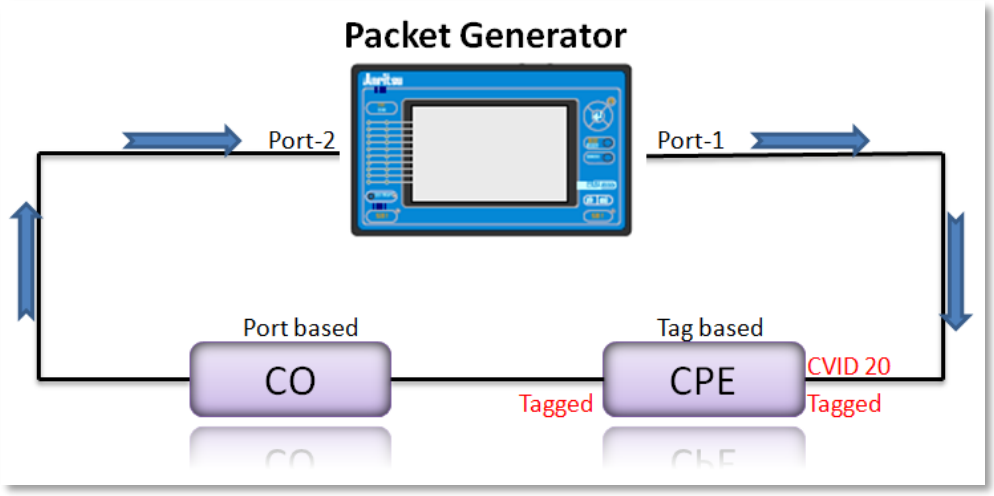


Figure 5-80 VLAN Test Result – 3

Data Direction: Port 1 --> Port 2

Port 1	**Port 2**
Untagged	81000014
Tagged 20 (81000014)	81000014
Tagged 100 (81000064)	**X**

Table 5-5 VLAN Test Result - 3

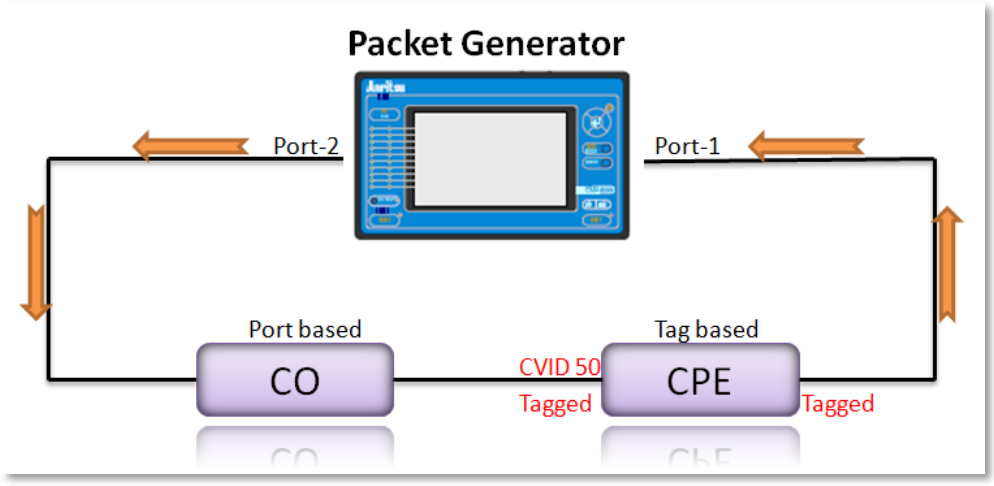


Figure 5-81 VLAN Test Result – 4

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

Table 5-6 VLAN Test Result - 4

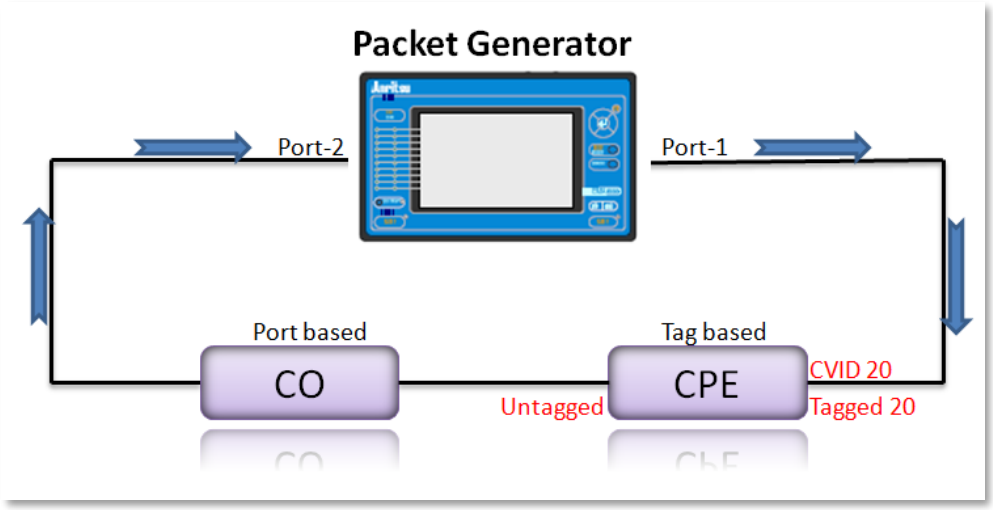


Figure 5-82 VLAN Test Result – 5

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

Table 5-7 VLAN Test Result - 5

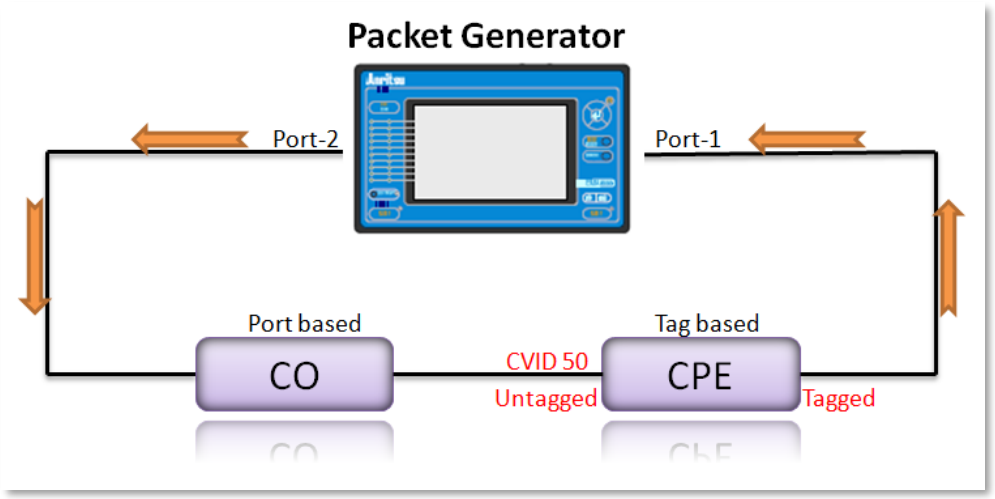


Figure 5-83 VLAN Test Result – 6

Data Direction: Port 2 --> Port 1

Port 2	**Port 1**
Untagged	81000032
Tagged 50 (81000032)	81000032
Tagged 100 (81000064)	**X**

Table 5-8 VLAN Test Result - 6

22.3. Basic Routing

Routing Application:

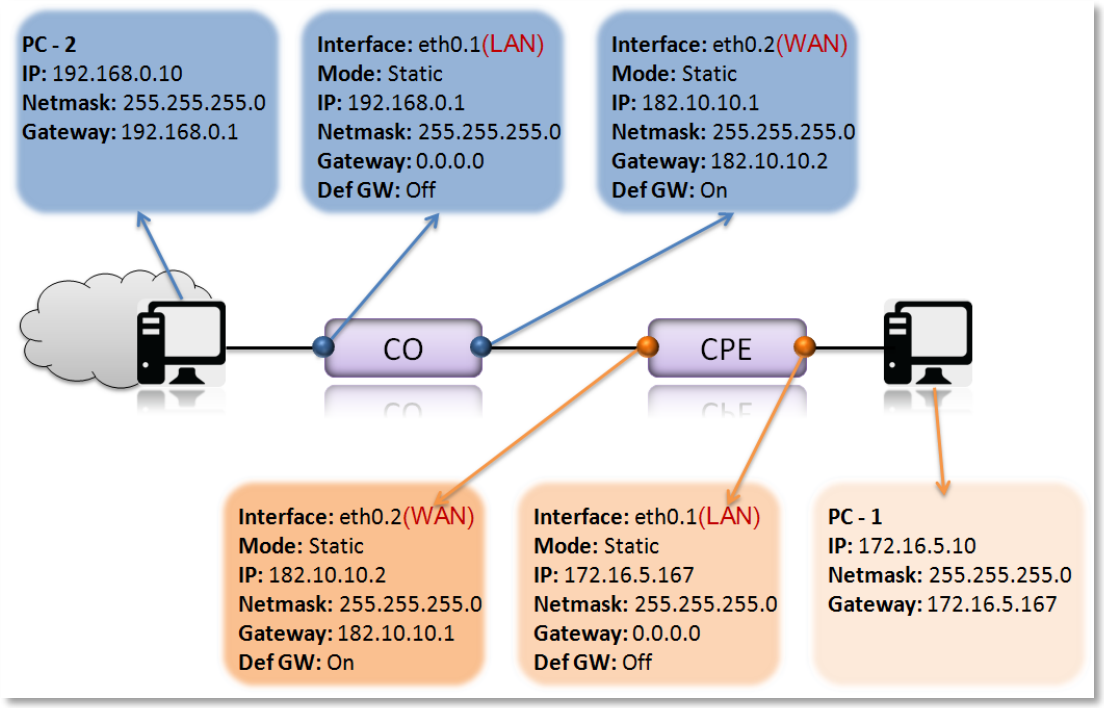


Figure 5-84 Routing Application

- < CO configuration >

1. Configuration > Local Setting > G.SHDSL

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

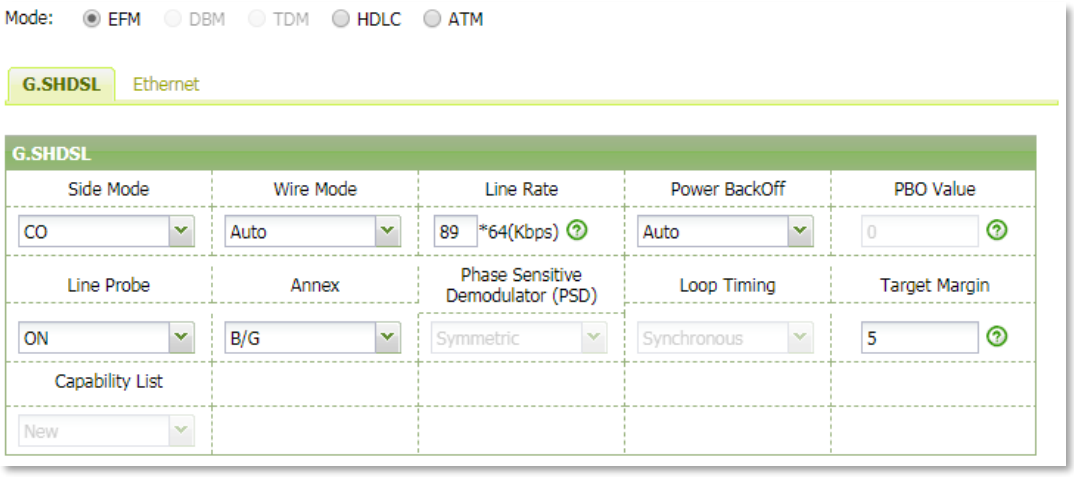


Figure 5-85 CO-G.SHDSL

2. Bridge / Routing > VLAN

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

All ports with **VLAN 2** are **untagged** for the WAN port.

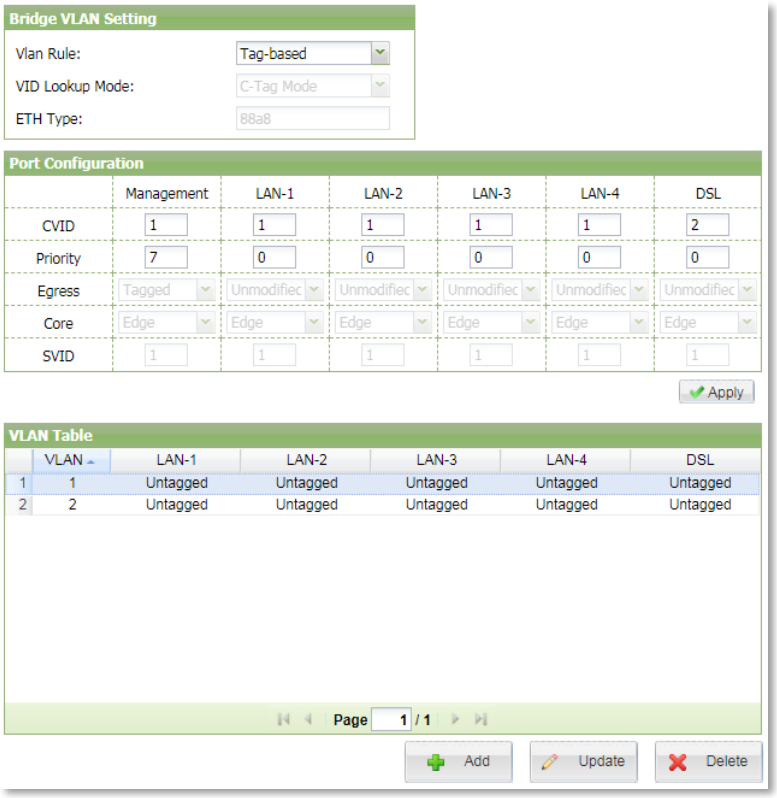


Figure 5-86 CO-VLAN

3. Bridge / Routing > Virtual IP

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

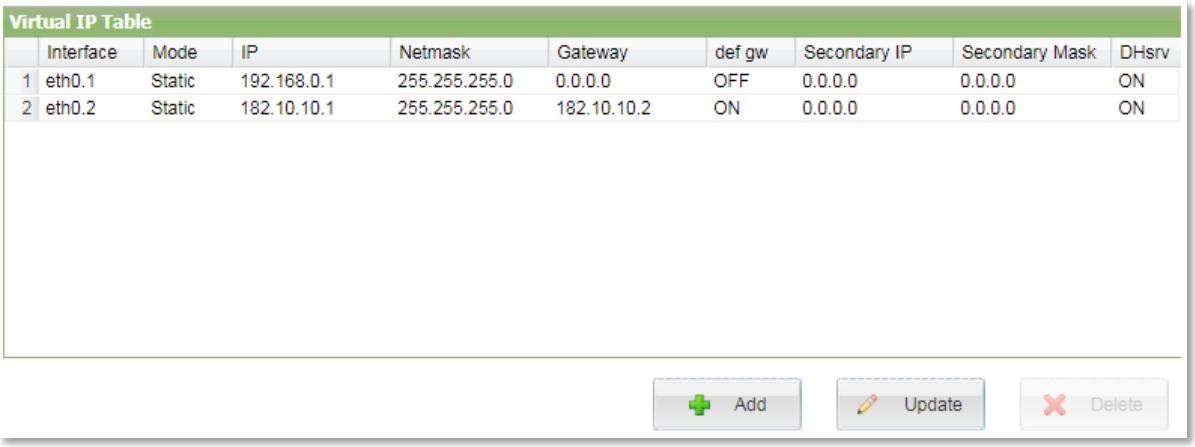


Figure 5-87 CO-Virtual IP

** Note: Remember to save after configuring.

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

The default master-slave relationship of ML634R 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.

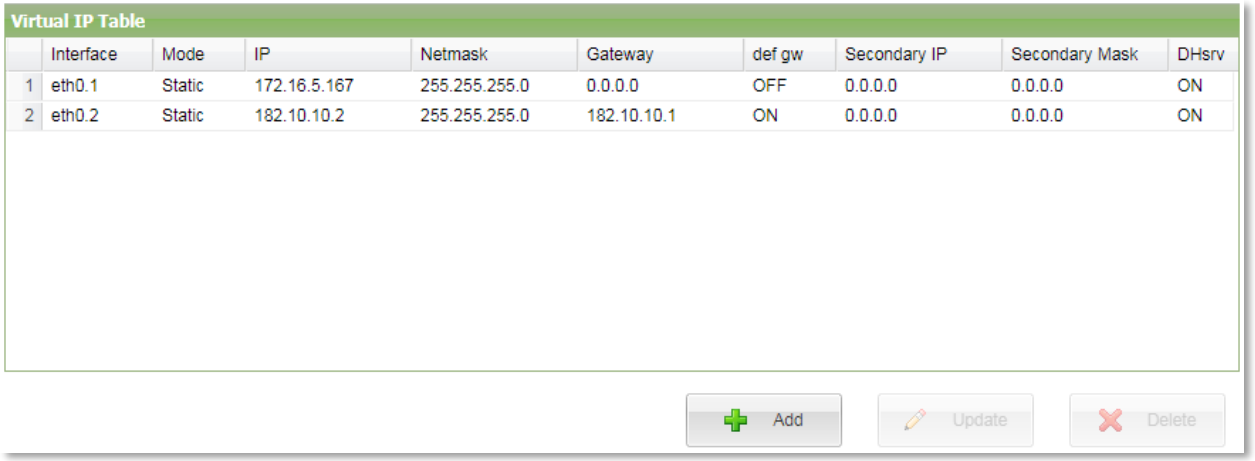


Figure 5-88 CPE-Virtual IP

** Note: Remember to save after configuring.

22.4. NAT Routing Application

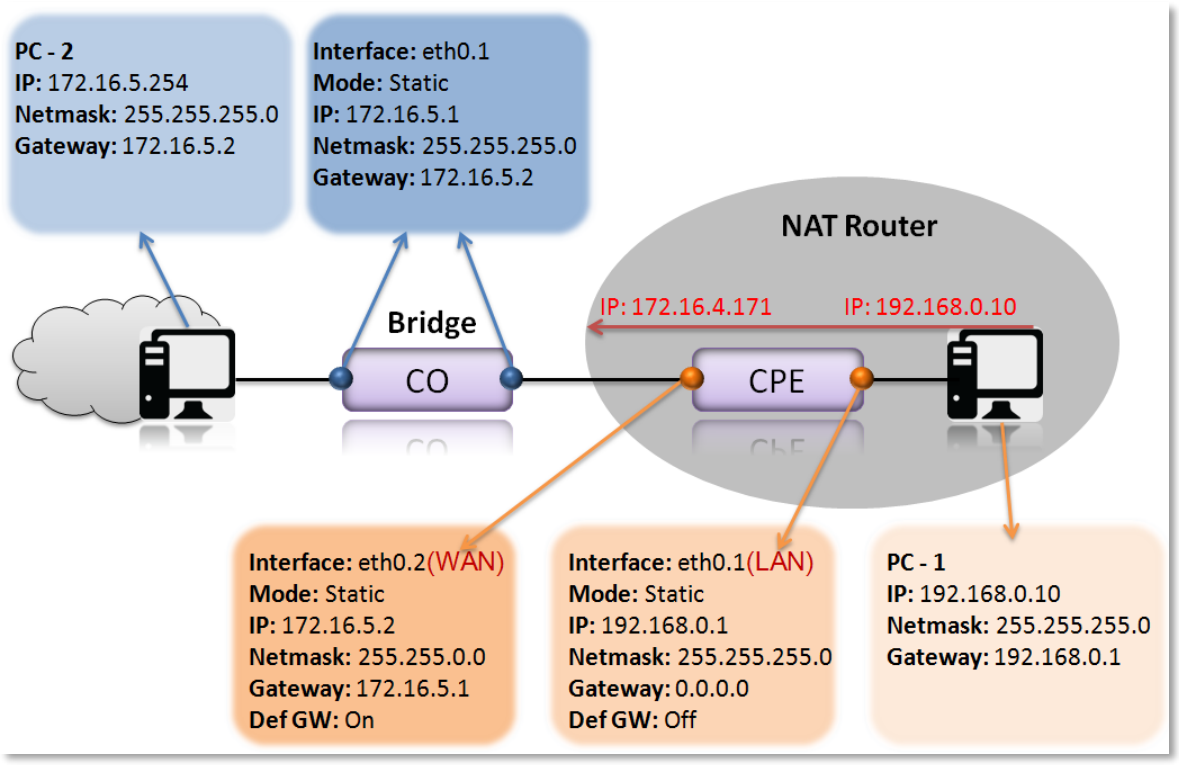


Figure 5-89 NAT Routing Application

- < CO configuration >

1. Configuration > Local Setting > G.SHDSL

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

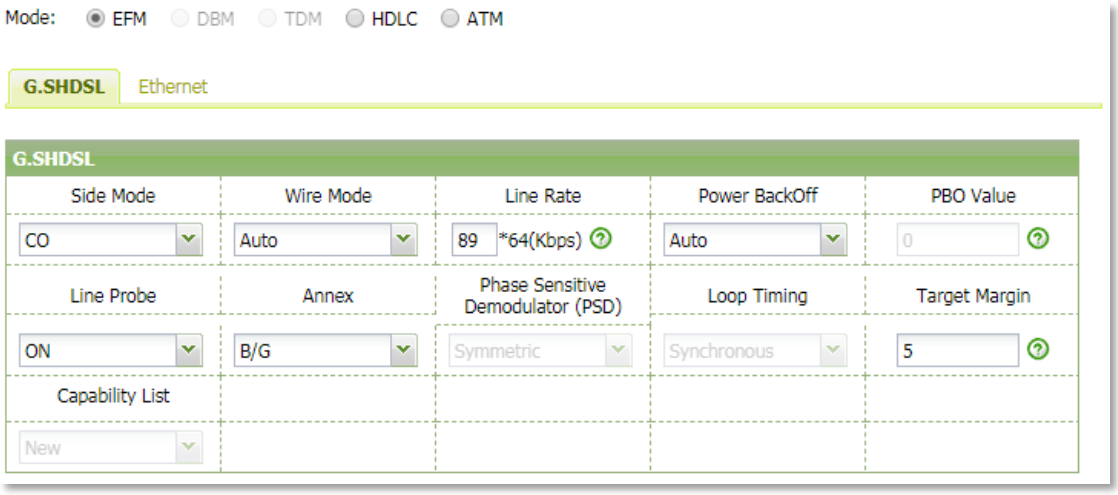


Figure 5-90 CO-G.SHDSL

2. Configuration > General Setup > Local

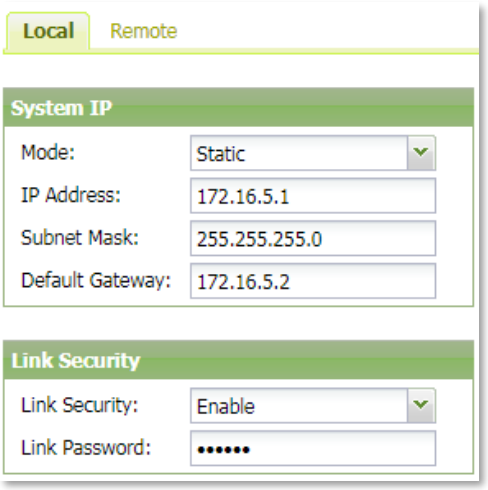


Figure 5-91 CO-General Setup

Note: Remember to save after configuring.

- < CPE configuration >

1. Configuration > Local Setting > G.SHDSL

The default master-slave relationship of ML634R 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**.

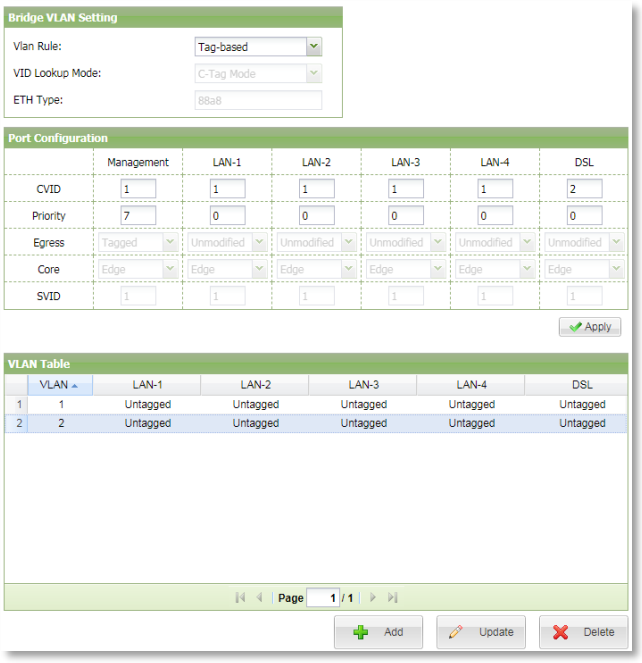


Figure 5-92 CPE-VLAN

3. Bridge / Routing > Virtual IP

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

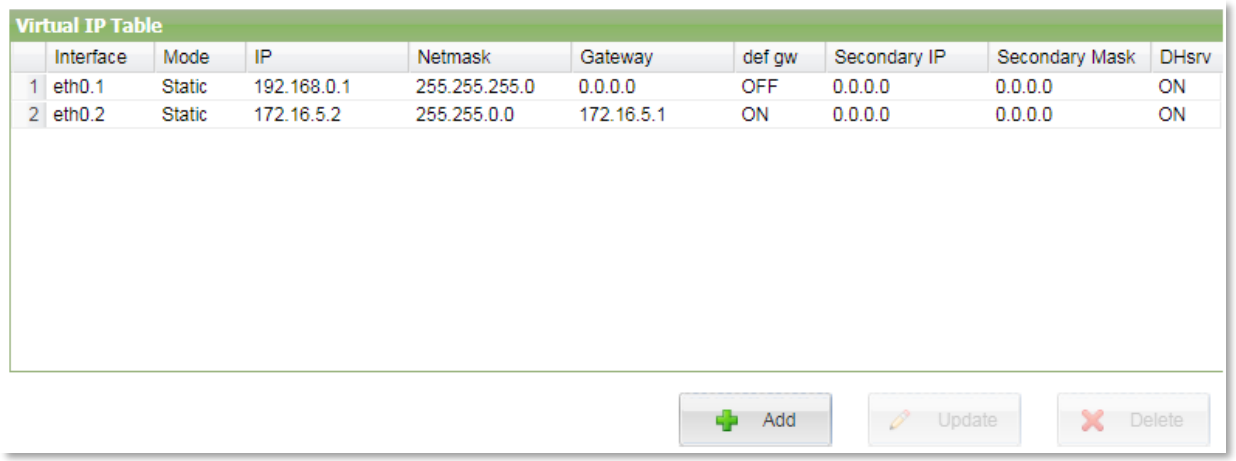


Figure 5-93 CPE-Virtual IP

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 the original IP.
- 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**

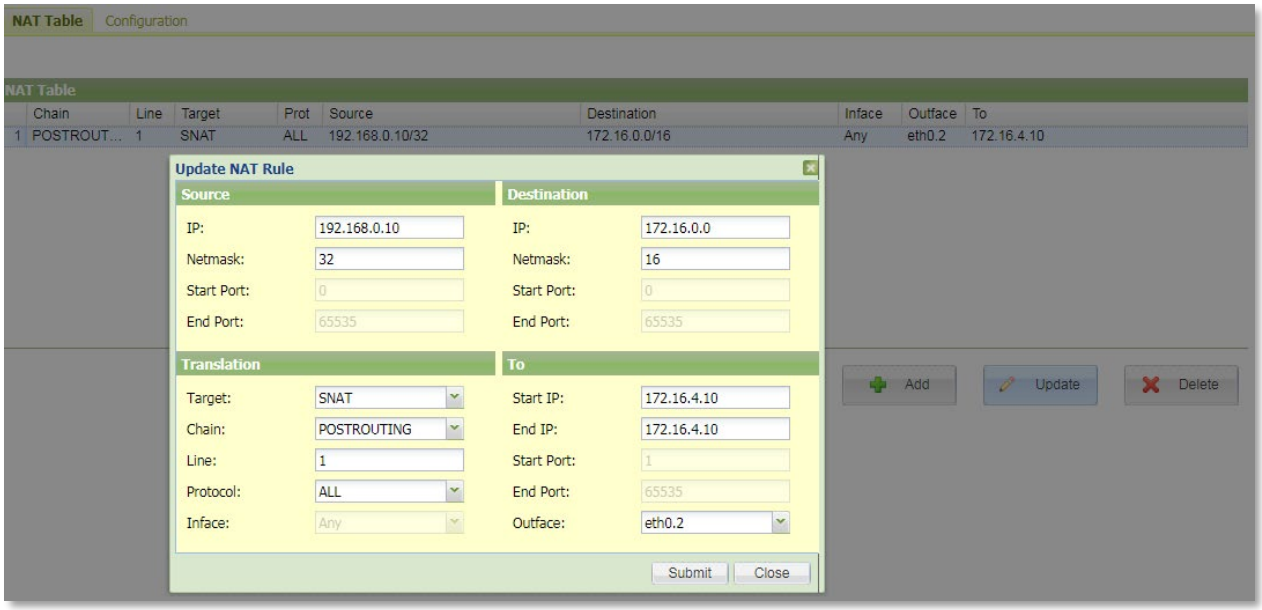


Figure 5-94 CPE-NAT Table

** Note: Remember to save after configuring.

22.5. VLAN Multiplexer Application

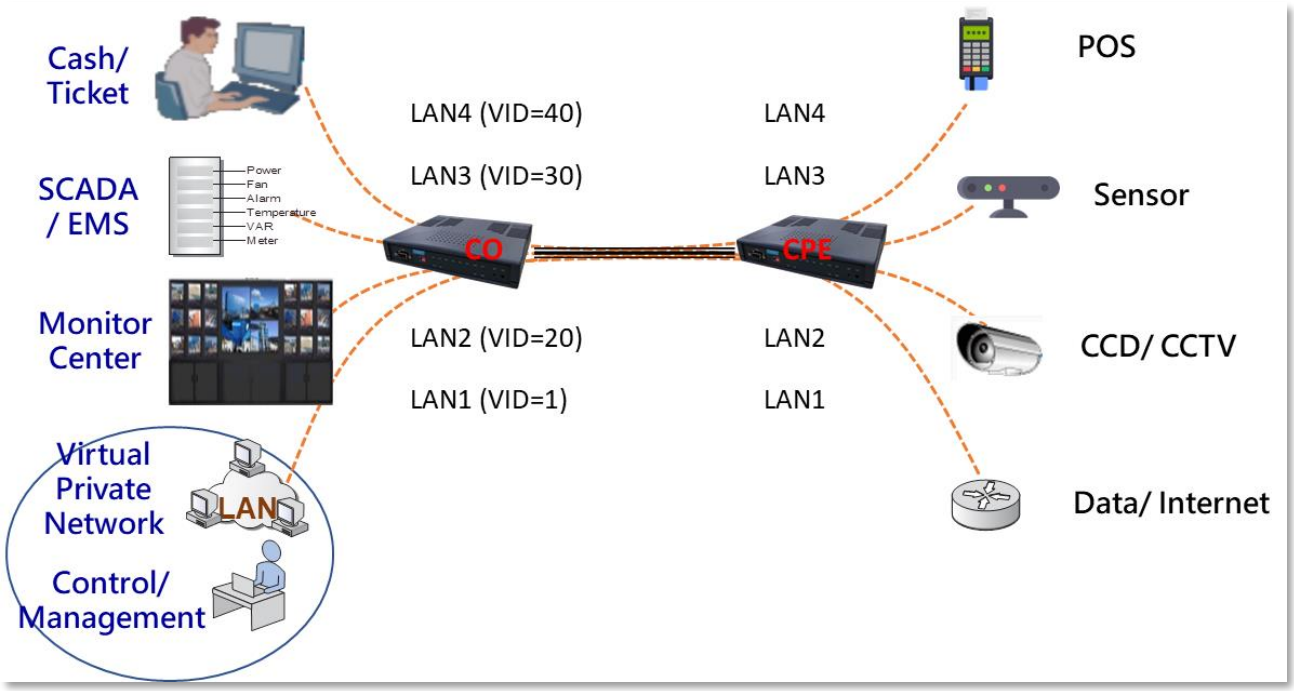


Figure 5-95 VLAN multiplexer application

Application:

Use G.SHDSL as a long-distance Ethernet Bridge that separates four different applications by different LAN port connections. Each LAN port has its own traffic which is isolated from other LAN ports.

Configuration:

Control/ Management PC IP address: 192.168.0.170

ML630R at CO IP address: 192.168.0.108

ML630R at CPE IP address: 192.168.0.109

Default Login User Name: admin

Default Login Password: admin

ML630R default IP address: 192.168.0.1

1. To simplify the configuration, all configuration starts by loading the factory default:

   [Maintenance]→[Software Default]→[Apply]

Figure 5-96 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]

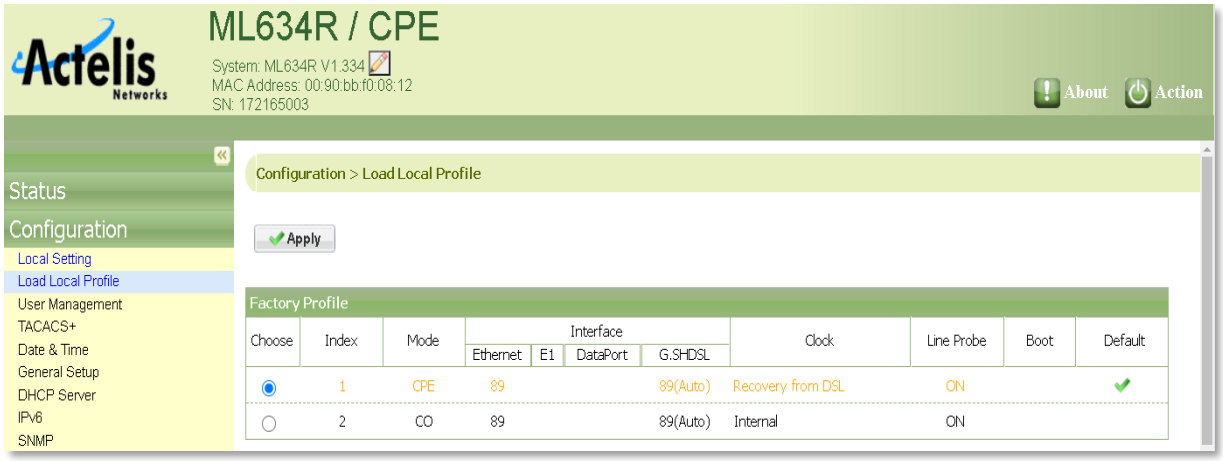


Figure 5-97 Load factory CPE default profile

4. On the CO site, change the IP address to 192.168.0.108

   [Configuration]→[General Setup]→Local [System IP] →[IP address] →192.168.0.108

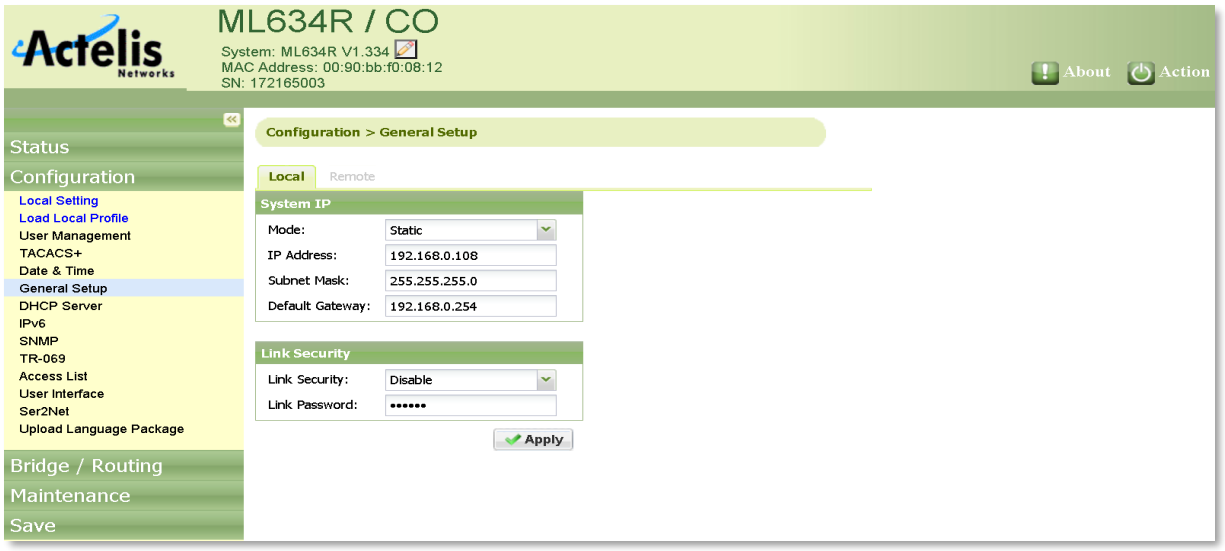


Figure 5-98 Change IP address of CO device

5. On the CPE site, change the IP address to 192.168.0.109

   [Configuration]→[General Setup]→Local [System IP] →[IP address] →192.168.0.109

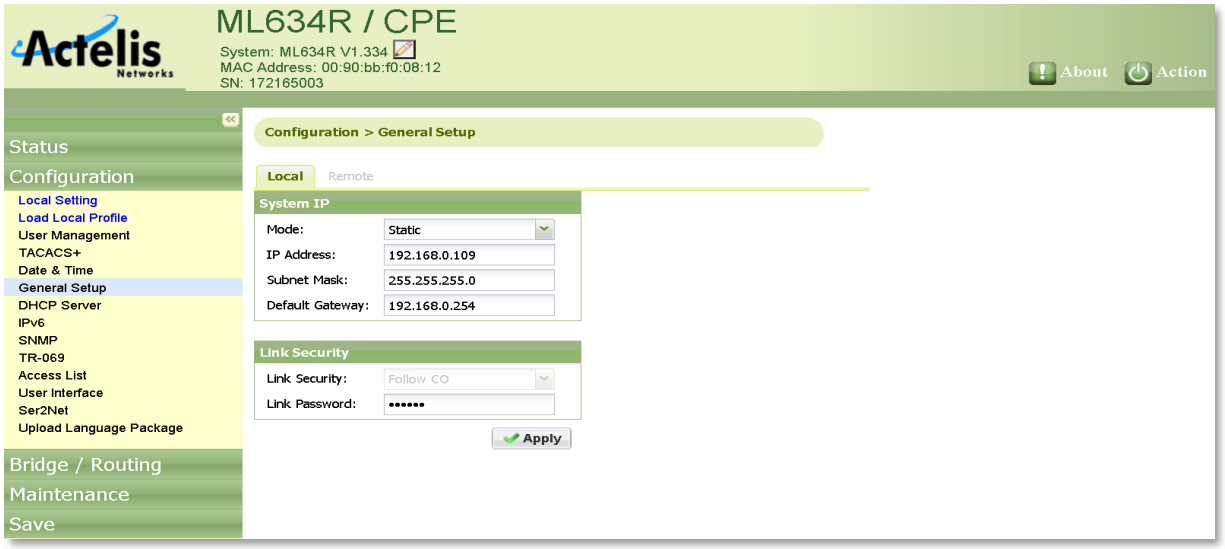


Figure 5-99 Change IP address of CPE device

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

   [Bridge/ Routing] → [VLAN] → [VLAN Rule] → Tag-based → [Apply]

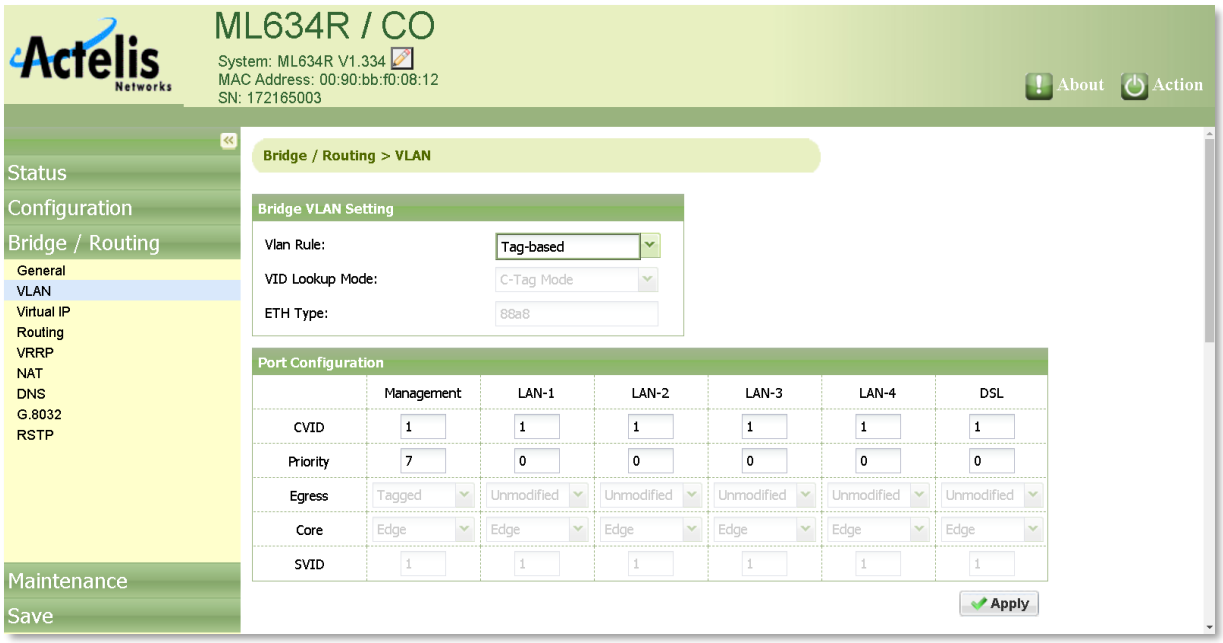


Figure 5-100 Apply Tag-based VLAN rule

7. Edit the VLAN table; the VLAN table will be displayed after Tag-based rule has been selected

   [Bridge/ Routing] → [VLAN] →[VLAN Table]→1 →[Update]

Figure 5-101 Setup VLAN Table configuration

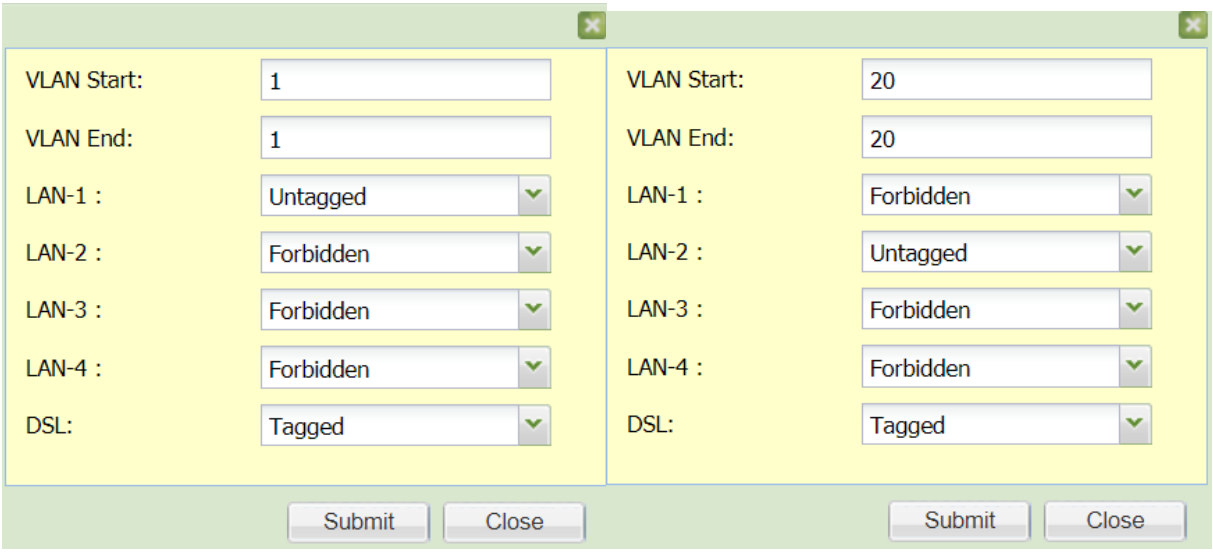


Figure 5-102 Setup VLAN rule of VID 1 and 20

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

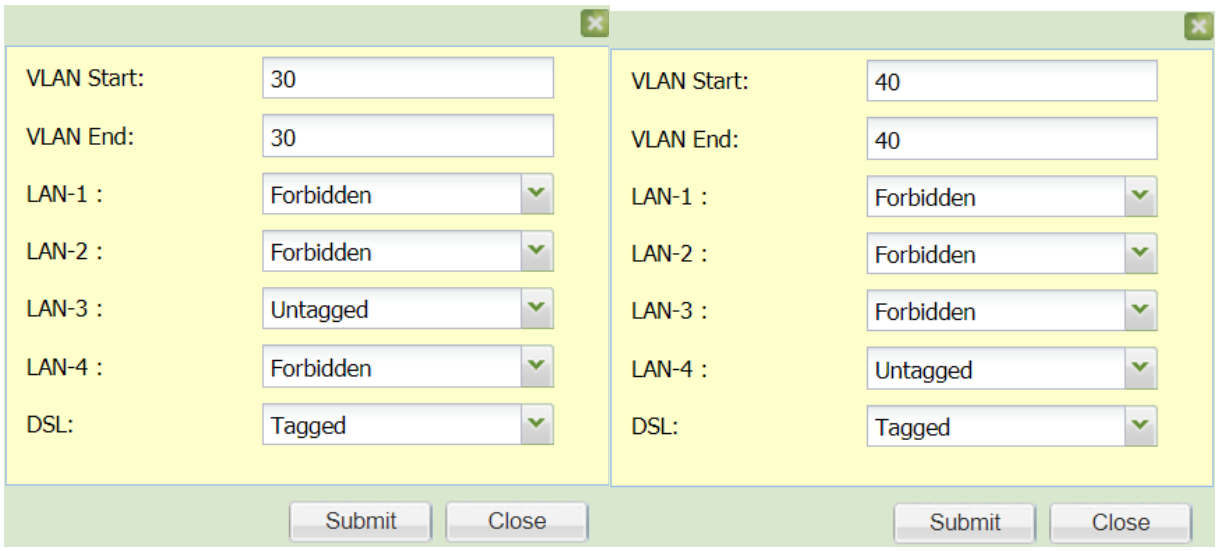
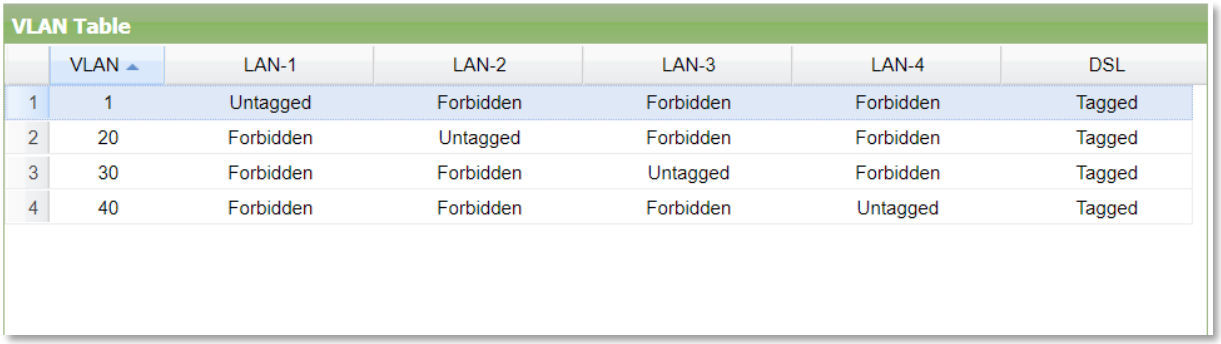


Figure 5-103 Setup VLAN rule of VID 30 and 40

[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 5-104 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]

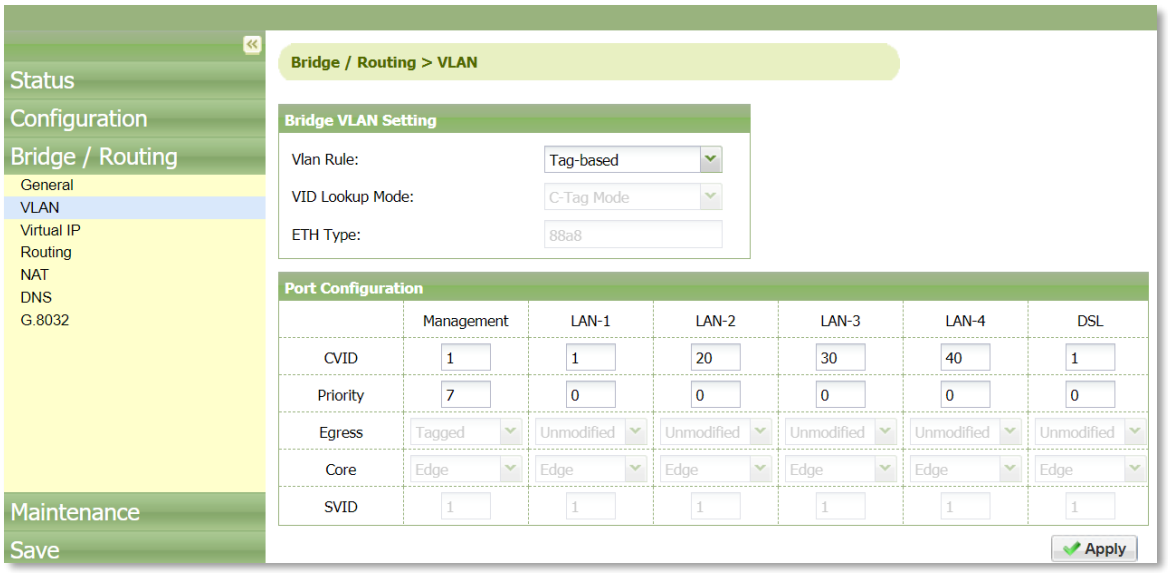


Figure 5-105 Setup the Core port VID

9. [Save]→[Local Save]→SHDSL→[OK]

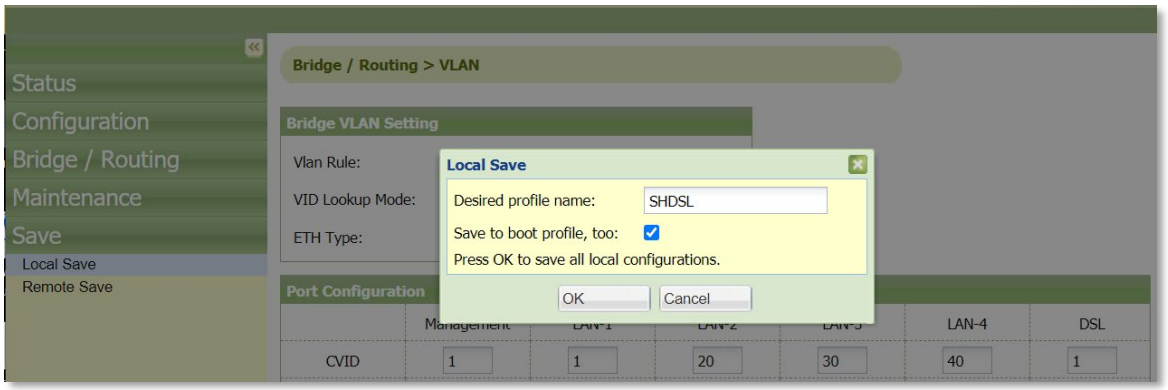


Figure 5-106 Save the working configuration to profile

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

Notes:

1. In order to prevent loss of management control it is important to perform steps 6, 7 and 8 in that order.
2. The default username and password is easily hacked. Please remember to change it before deployment.
3. Changing the VLAN Rule to [Tag-based] in the Bridge/ Routing group will also change the System IP setting from Configuration/[General Setup] to Bridge/ Routing [Virtual IP].

VI. CLI Operation

This Chapter describes the ML630R Command Line Interface. There are two methods to access the Command Line Interface: the Craft port and Telnet, both of which provide the same command format. 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 Command Line Interface by using Telnet software to remotely control or maintain the device from anywhere in the global IP network. The following introductions are based on the ML630R with firmware version ***v1.371****.*

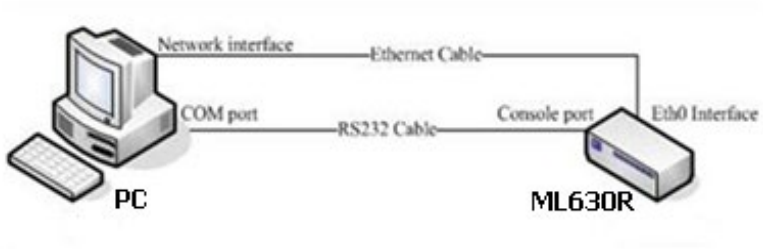


Figure 6-1 Basic Management Connection

23. Connection via Craft Port

By using a VT-100/ANSI compatible terminal emulation software, such as Microsoft HyperTerminal or Tera Term, users can configure the ML630R via the Craft port with a 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**

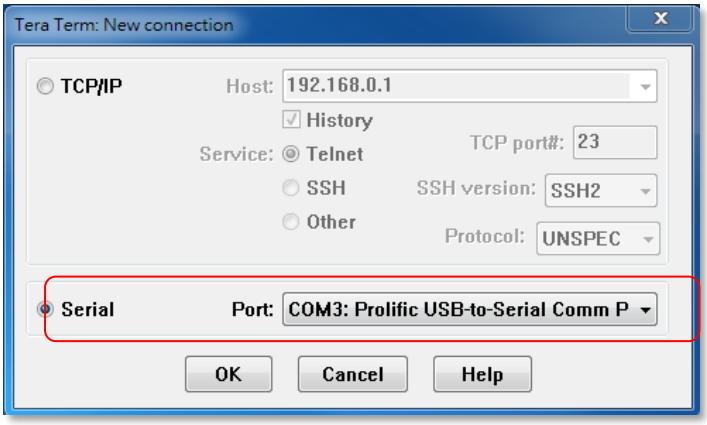


Figure 6-2 Select the correct Series Port in Tera Term

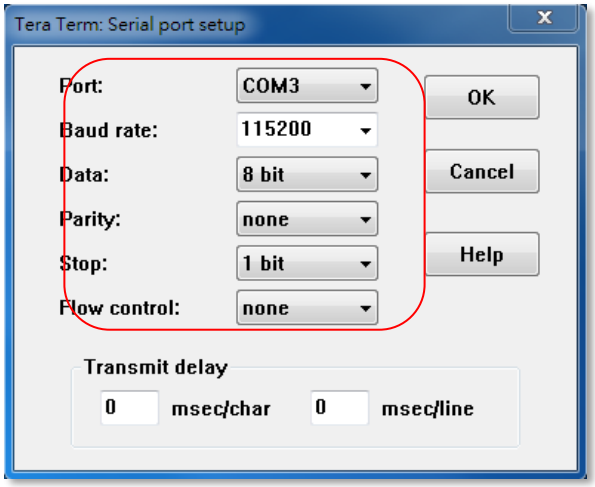


Figure 6-3 Series Port Parameters

24. Connection via Telnet/SSH Protocol

The ML630R default IP address is shown below. Users can update the 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

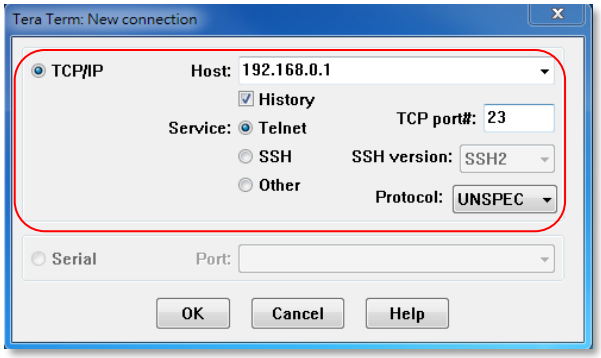


Figure 6-4 Select Telnet/SSH with correct IP

25. The Command Line Interface

After connecting to the ML630R, the terminal UI will display the Root Menu as shown below. The user has to input the correct user name and password for the login process. The default highest authority is admin/admin.

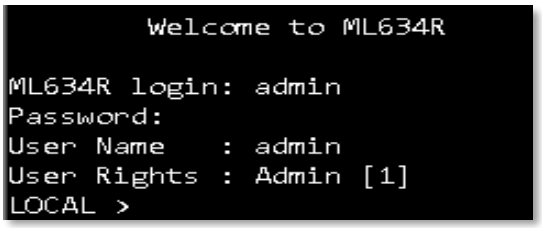


Figure 6-5 Login Screen of Actelis

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

Figure 6-6 Main Command Lines

25.1. “aclset” Command

This command is used to set ACL. ML630R supports two methods, “**normal**” and “**white list**” with different match conditions to filter specified data packets.

```
LOCAL >acls

---------- 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
                 [ 6:OPT2, 5:OPT1, 2:UTP2, 1:UTP1, bit0:CPU]
        -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)]

 Example (normal mode: 40 rules):
                1. Set Mac filter(Deny 00:90:bb:xx:xx:xx destination mac from all port).
           acls -y 1 -f 0 -t 66 -d 00:90:bb:00:00:00 -n ff:ff:ff:00:00:00
                2. Set IP filter (drop source IP of range(192.168.0.x)from all port).
           acls -y 1 -f 1 -t 66 -s 192.168.0.0 -m 255.255.255.0
                3. Set Destination Port filter (drop destination port 21).
           acls -y 1 -f 3 -t 66 -p 21 -k ffff
-----------------------------------------------------------------
 Example (white list mode: 8 rules):
                1. Block invalid Source IP except 192.168.0.21 and 192.168.0.25
                        acls -y 2 -f 1 -s 192.168.0.21 -m 255.255.255.255
                        acls -y 2 -f 1 -s 192.168.0.25 -m 255.255.255.255
                2. Block invalid Source IP except 192.168.0.240~254 and 192.168.0.22
                        acls -y 2 -f 1 -s 192.168.0.240 -m 255.255.255.240
                        acls -y 2 -f 1 -s 192.168.0.22 -m 255.255.255.255
                3. Block invalid Source IP except 172.16.5.100/8 and destination port 22
                        acls -y 2 -f 2 -s 172.16.5.100 -m 255.0.0.0 -p 22 -k ffff
                4. Block invalid destination except port0 to port21
                        acls -y 2 -f 3 -p 0 -q 21
-------------------------------------------------------------
                Delete index 2 acl rule.
                        acls -N 2
```

Figure 6-7 “aclset” Command

25.2. “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

25.3. “arp” Command

Input this command to get the ARP table with options to filter entries matching 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

25.4. “atmset” Command

This command is used to set the ATM parameters. This command can only be used of the G.SHDSL mode is configured as ATM.

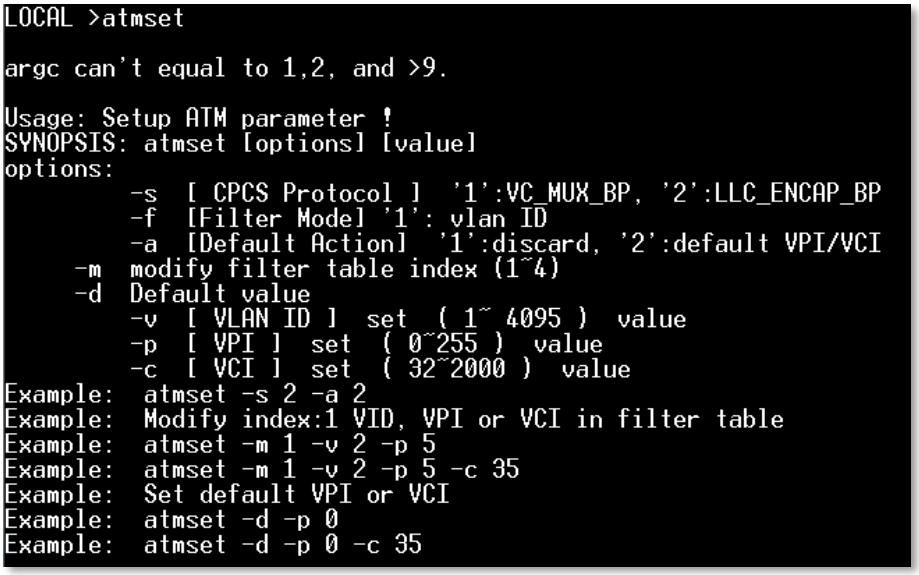


Figure 6-10 "atmset" Command

25.5. “atmget” Command

This command is used to check ATM functions, 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

25.6. “briget” Command

This command is one of the most important commands for routing applications. Users are able to check the 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:
    -c          Show Configuration
    -p          Show Port Forwarding Member
    -m          Show Mac Table
    -v          Show VLAN Table
```

Figure 6-12 “briget” Command

25.7. “briset” Command

This command is used to set VLAN parameters. There are three main VLAN rules, such as tag based, port based and Q-in-Q.

- **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

25.8. “communityset” Command

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

Figure 6-14 “communityset” Command

25.9. “communityget” Command

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

Figure 6-15 “communityget” Command

25.10. “dhget” Command

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

Figure 6-16 “dhget” Command

25.11. “dhset” Command

This command is used to set the DHCP parameters, 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”.

```
LOCAL >dhset

---------- CLI_DHCP_SET_Help ---------------
 Usage   : Set DHCP Server
 Synopsis:
    dhset [Options] [-u -i -m]
 ============================================
 Options:
    -o          [0~2]      Server Mode 0:Off, 1:Server, 2:Relay
    -r          [IPv4]     Relay Server IP
    -v          [1~4094]   Relay Interface VLAN
    -s          [IPv4]     Start IP
    -e          [IPv4]     End IP
    -n          [IPv4]     NetMask
    -g          [IPv4]     Gateway IP
    -l          [0~255]    Max Lease
    -w          [60~86400] Lease Time (sec)
    -t          [IPv4]     NTP Server
    -N          [String]   Domain Name (length:32)
    -D          [IPv4]     DNS Primary Server
    -d          [IPv4]     DNS Secondary Server

    -u          [0~19]     Updtae Index to Static Leases
    -i          [IPv4]     Static Lease IP
    -m          [MAC]      Static Lease MAC
 Example:
    1. add rule
       dhset -i 192.168.0.12 -m 00:aa:bb:cc:dd:ee
    2. delete rule 1
       dhset -u 1
    3. update ip in rule 1
       dhset -u 1 -i 192.168.0.13
```

Figure 6-17 “dhset” Command

25.12. “dnsget” Command

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

```
LOCAL >dnsget

---------- CLI_DNS_GET_Help ---------------
 Usage   : Get DNS Configuration
 Synopsis:
    dnsget [Options]
 ============================================
 Options:
    -a          Show DNS all settings
    -d          Show DNS Cache settings
    -m          Show DNS Authoritative Server settings
```

Figure 6-18 “dnsget” Command

25.13. “dnsset” Command

This command is used to set the DNS configuration.

```
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

25.14. “exit” Command

Input “**exit**” to log out the system.

```
LOCAL >exit
CLI_EXIT



        Welcome to ML634R

ML634R login:
```

Figure 6-20 “exit” Command

25.15. “fmget” Command

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

```
LOCAL >fmget

Usage: GET FM       !
SYNOPSIS: fmget  [-c,-a,-r]
            c - Set clear alarmlog
            r - GetRealTimeAlarm
            a - GetAlarmLog
Example:
                fmget  -a
```

Figure 6-21 “fmget” Command

25.16. “gset” Command

This command is used to set G.SHDSL parameters, such as CO/CPE mode, line rate, wire mode, line probe, EFM/ ATM mode and so on.

```
LOCAL >gset

Usage: Setup SHDSL 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
        -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
Example:    gset  -m 0  -x 1
```

Figure 6-22 “gset” Command

25.17. “get” Command

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

```
LOCAL >get
------------------------------------------------------------------------
---------------------  show G.shdsl /LAN parameter  ---------------------
    configuration
------------------------------------------------------------------------
    G.shdsl Mode        CPE
    G.shdsl Wire        Auto
    G.shdsl Linerate       89
    G.shdsl Pbo         Enable
    G.shdsl Pscale          0 dB
    G.shdsl Psd         Sync
    G.shdsl Annex       Annex-B/G
    G.shdsl lineprobe   Enable
    G.shdsl SNR Margin      5 dB
    G.shdsl RefClock    mode 3a
    G.shdsl mode   EFMonly
    G.shdsl Extended Mode  Disable
    G.shdsl Extended PAM   128_PAM
    G.shdsl Extended MaxRate 213
    G.shdsl Bonding Header   Enable
    G.shdsl AtnThres       40 dB |   SnrThres                5 dB
    G.shdsl CRC_Thres       2
    G.shdsl Capability List Style   NEW
------------------------------------------------------------------------
```

Figure 6-23 “get” Command

25.18. “rpget” Command

This 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

25.19. “rpset” Command

This command is used to set G.8032 function. The “**-a**” parameter can initially be used to see all the information. Depending on whether the topology is a DSL/ Ethernet ring topology or a DSL serial linear network, some parameters may, or may not, be relevant.

```
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

25.20. “ipset” Command

This command is only effective in Bridge mode. Users can configure the IP network parameters.

```
LOCAL >ipset

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

parameter error
```

Figure 6-26 “ipset” Command

25.21. “ipv6get” Command

This 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

25.22. “ipv6set” Command

This command is used to manually configure the IPv6 parameters, including 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

25.23. “lanset” Command

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

```
LOCAL >lanset

Usage: Setup LAN parameter !
SYNOPSIS:
lanset [Port] [-a,-s,-f,-i,-e,-w] [value]
              port number                    [1 ~ 4]
Options: Port - port identifier
   a - AdminStatus,            [1]:Enable, [0]:Disable
   s - LanSpeedMode
      [4]:100-full,[3]:100-half, [2]:10-full, [1]:10-half, [0]:AutoNegotiation
   f - Flow Control,                          [0]:turn off, [1]:turn on
 ------------------------------------------------------------------------
   i - ingress_rate setting , [0]:turn off, [1]:64kbps, [2]:128Kbps, [3]:256kbps
       [4]:512kbps,[5]:1Mbps, [6]:2Mbps, [7]:5Mbps, [8]:10Mbps
       [9]:20Mbps,[10]:50Mbps
   e - egress_rate setting , [0]:turn off, [1]:64kbps, [2]:128Kbps, [3]:256kbps
       [4]:512kbps,[5]:1Mbps, [6]:2Mbps, [7]:5Mbps, [8]:10Mbps
       [9]:20Mbps,[10]:50Mbps
   w - AlmSwitch,       [1]:Enable, [0]:Disable
Example: ---------------------------------------------------------------
                lanset 1 -a 1 -f 1
                lanset 1 -s 2
------------------------------------------------------------------------
```

Figure 6-29 “lanset” Command

25.24. “langet” Command

This command is used to check all LAN parameters.

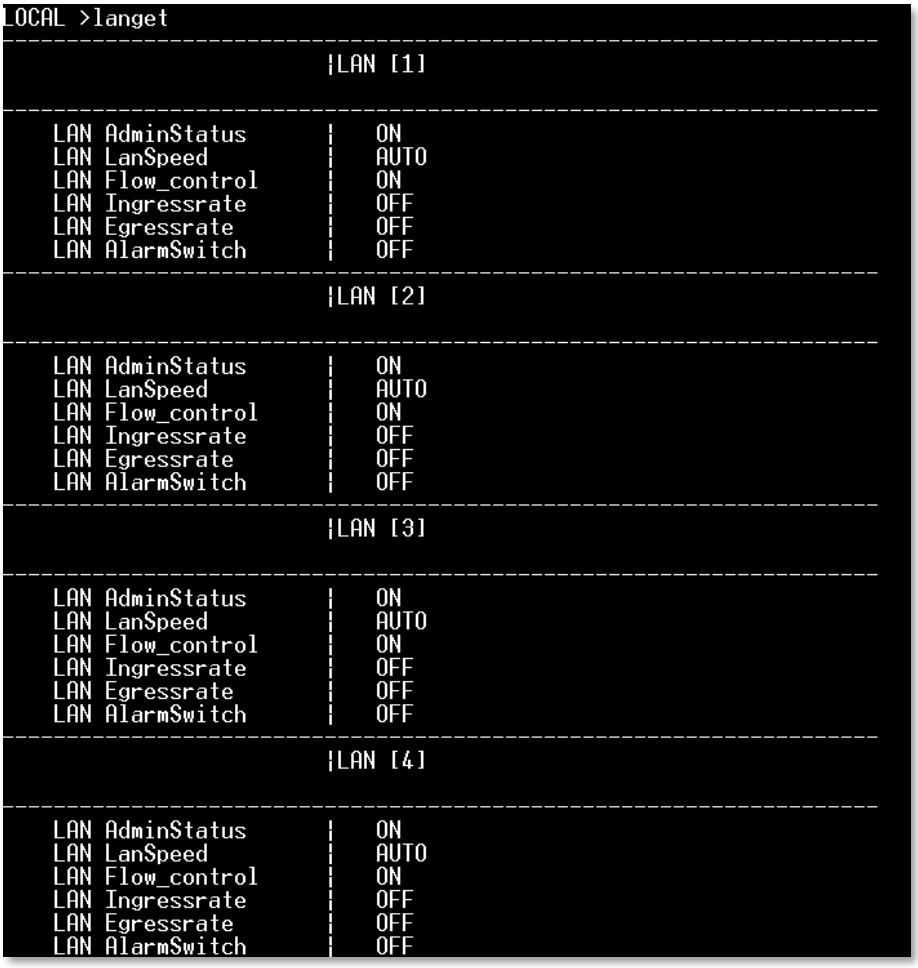


Figure 6-30 “langet” Command

25.25. “load” Command

This command is used to load the factory or default file, allowing users a more convenient way to establish the DSL connection.

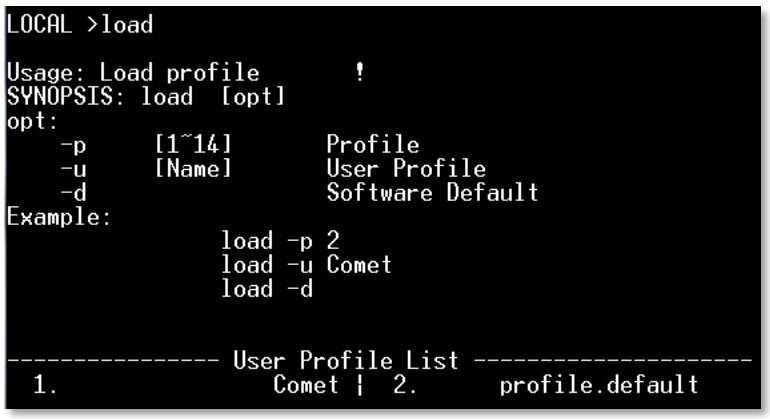


Figure 6-31 “load” Command

25.26. “maclg” Command

This command is used to display the MAC learning table for all ports.

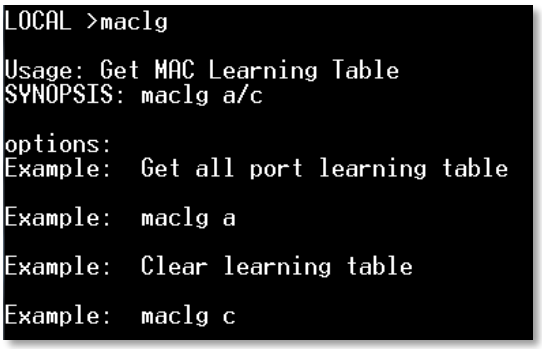


Figure 6-32 “maclg” Command

25.27. “natget” Command

This 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

25.28. “natset” Command

This command is used to set the NAT function. There are three main NAT items, “**SNAT**”, “**MASQURADE**” and “**DNAT**”. Different NAT definitions have different rules which need 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

25.29. “pmset” Command

This command is used to clear all G.SHDSL performance records.

```
LOCAL >pmset

Usage: Setup PM parameter !
SYNOPSIS: pmset [TYPE][-a, -m, -d, -q, -s]
TYPE:  -g : GSHDSL  -e E1Options:    a- clean_all,         m- clean_Current15min
           d- clean_Current1Day, q- clean_History15min
           s- clean_History1Day
Example:
               pmset  -g -a    --Clear Gshdsl all PM record
               pmset  -e -s    --Clear E1 1Day History PM record
```

Figure 6-35 “pmset” Command

25.30. “pmget” Command

This command is used to check all G.SHDSL performance records.

```
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

25.31. “ping” Command

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

```
LOCAL >ping

---------- CLI_PING_Help ---------------
 Usage   : ping
 Synopsis:
    ping [IPv4] -v [1~4094]
 ============================================
```

Figure 6-37 “ping” Command

25.32. “run” Command

This command is used to run all settings immediately.

Figure 6-38 “run” Command

25.33. “remote” Command

If 2 ML630R are connected as local and remote modems, “**remote**” will access the remote modem via EOC management, or **“local”** will revert to the local configuration.

Figure 6-39 “remote” Command

25.34. “rmon” Command

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

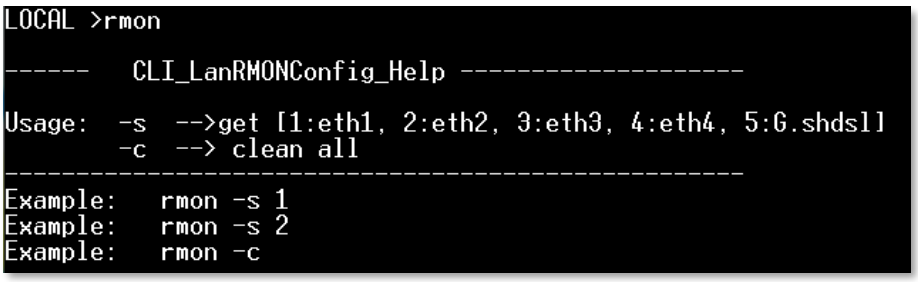


Figure 6-40 “rmon” Command

25.35. “sysset” Command

This command is used to set the system information, such as the system time, link security, system name, description, contact and location. Invoking the “sysset –r” command may reset the device and reload the saved profile.

```
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
       -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
       -i       [String] System Description (length:32)
       -o       [String] System Contact (length:64)
       -n       [String] System Name (length:32)
       -j       [String] System Location (length:128)

Example :
  * Set system time
    sysset -d 2016-08-18-12-34-561
```

Figure 6-41 “sysset” Command

25.36. “sysget” Command

This command is used to verify the system information. In general, users can check the IP network parameters within Bridge mode, the MAC address and other system parameters.

```
LOCAL >sysget
---          ML634R(Card:Yes)          ---
Link Security State : [ Disabled ]

[Switch Mode]System IP Configuration :
IP address : 192.168.0.1
NetMask    : 255.255.255.0
Gateway    : 0.0.0.0

DHCP Client : OFF

MAC Address:00:90:bb:f0:08:12
Transmit Clock Source : [ Internal ]
Clock Auto Switch : Off

System Local Time : 1970-01-01 02:28:18  GMT+00:00
NTP Admin         : OFF
NTP Server        : 0.0.0.0
Daylight Saving   : OFF

Serial Number     : 172165003
Software Version  : V1.334
Kernel Version    : 2018.08.24.1.7118
U-Boot Version    : 1.0.13
PCB Version       : V1.0
FW_VER(IDC)       : 2.1.0_00
PMD_VER(SDFE)     : 1.1-2.1.0__
FeatureStr        : TF-|AX+|SL+|BA-|EO-|MP+|

Description       : ML634R V1.334
Contact           :
Name              : ML634R
Location          :
LOCAL >
```

Figure 6-42 “sysget” Command

25.37. “show” Command

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

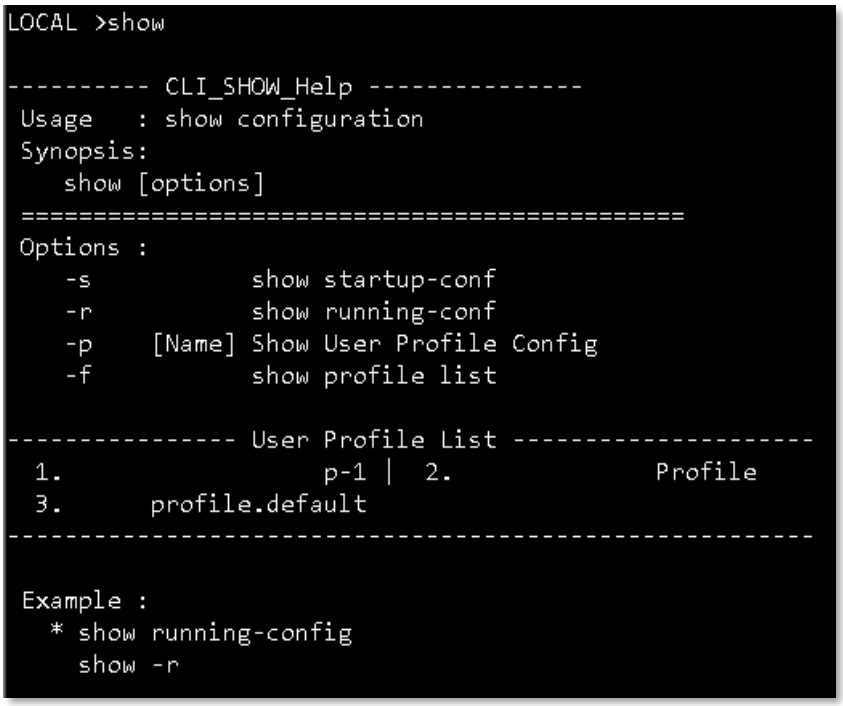


Figure 6-43 “show” Command

25.38. “status” Command

This command is used to check the G.SHDSL status. Typically network managers can use this command to check the DSL connection and current line rate.

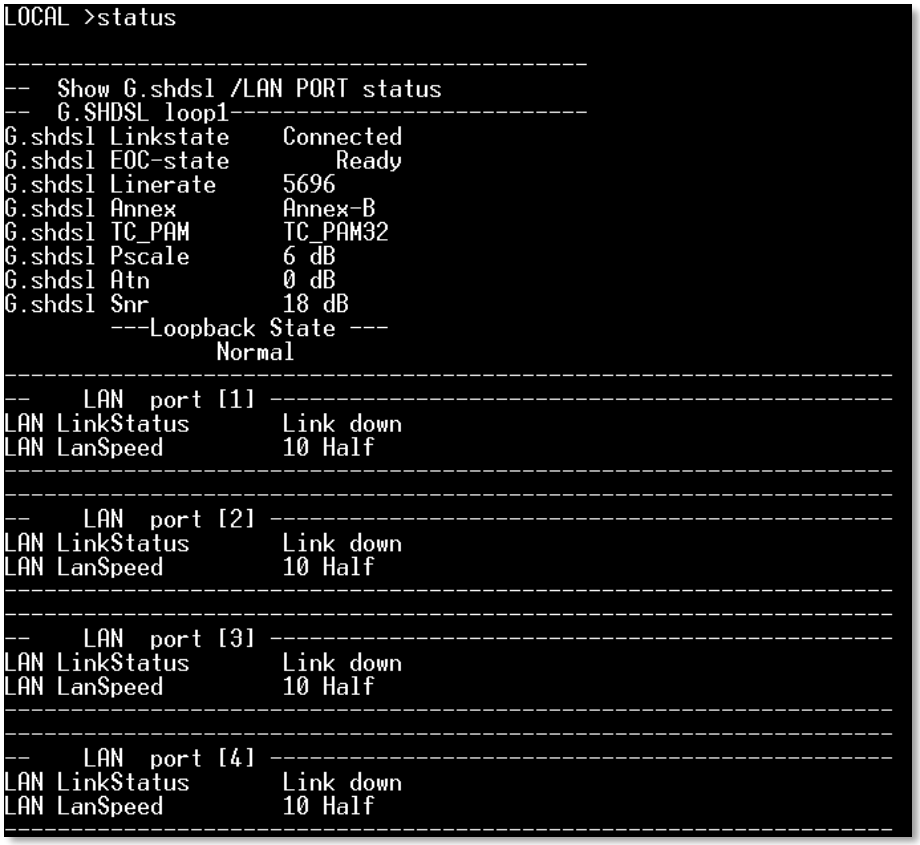


Figure 6-44 “status” Command

25.39. “snmpv3get” Command

This command is used to check the SNMPv3 parameters, such as user name, rights and security protocol.

Figure 6-45 “snmpv3get” Command

25.40. “snmpv3set” Command

This command is used to set SNMPv3 parameters including different security levels, passwords and algorithms which need 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

25.41. “save” Command

This command is used to save all settings after a change in configuration.

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

Figure 6-47 “save” Command

25.42. “tacget” Command

This 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

25.43. “tacset” Command

This command is used to set TACACS+ parameters.

```
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

25.44. “rstpg” Command

This command is used to get RSTP Parameters 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

25.45. "rstps" Command

This command is used to set RSTP parameters, 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

25.46. "tftp" Command

This command is used to download/ upload profile or upgrade the modem firmware via TFTP server. Users have to first prepare a workable TFTP server and place the firmware or configuration profile in the download path. One the file is available, it can be accessed by the ML630R by entering the correct IP, file path and file name.

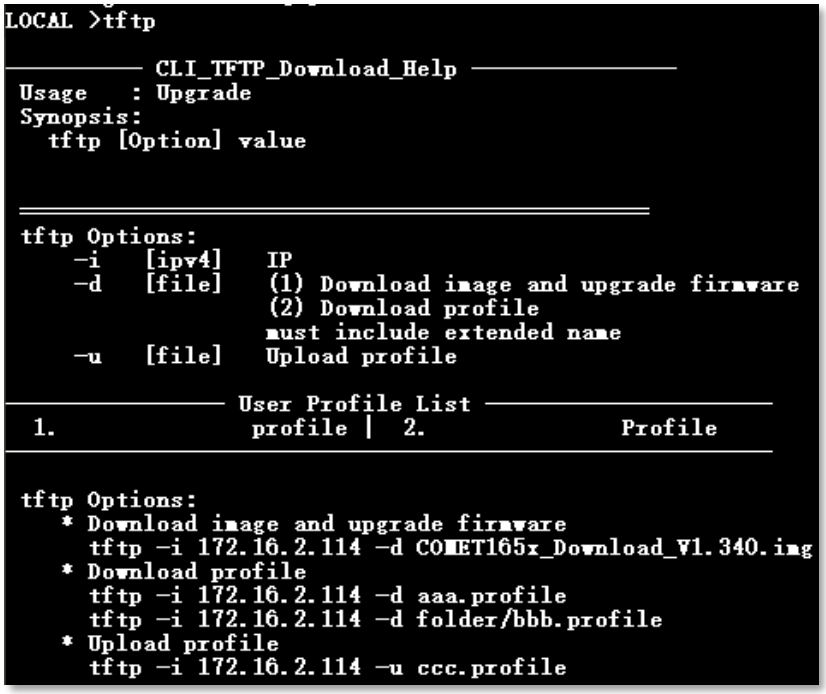


Figure 6-52 "tftp" Command

25.47. "tr069s" Command

This command is used to set TR-069 parameters. Modems act as TR-069 clients. In the protocol, clients have their own authentication, and need to match the server's configuration. Remember to check both sides use the same parameters.

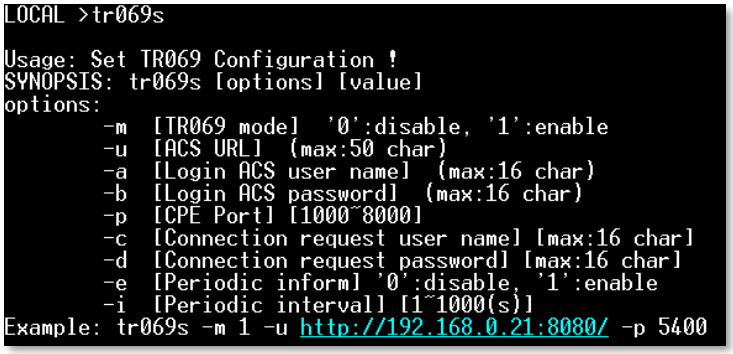


Figure 6-53 "tr069s" Command

25.48. "tr069g" Command

This 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
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
```

Figure 6-54 "tr069g" Command

25.49. "trapset" Command

This command is used to set the SNMP trap or Syslog 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

25.50. “trapget” Command

This command is used to display SNMP trap and Syslog IPs.

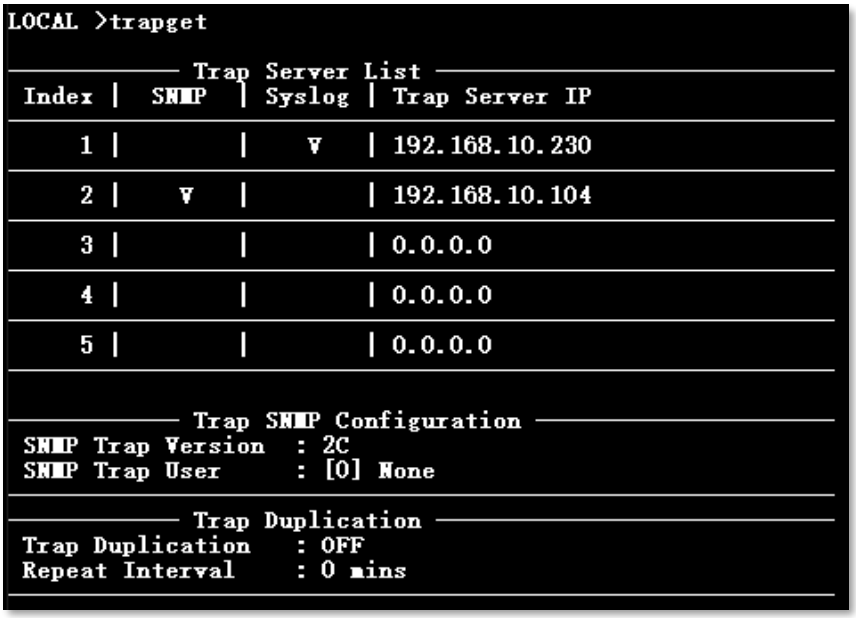


Figure 6-56 “trapget” Command

25.51. “userset” Command

ML630R supports three levels of security authority: “**Administrator**”, “**Operator**” and “**Monitor**”. Administrators are able to manage all functions, such as add, delete or modify. Password rules can also be configured.

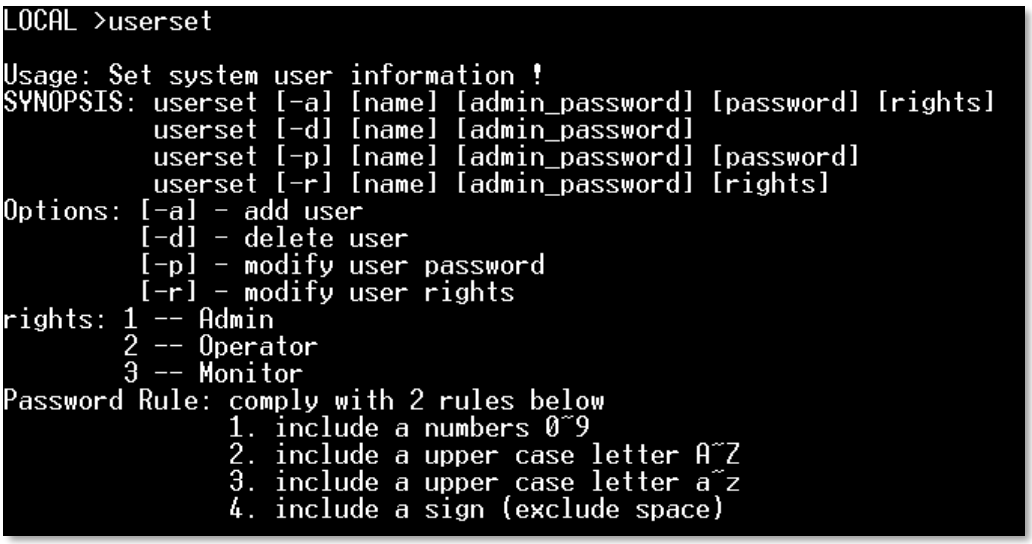


Figure 6-57 “userset” Command

25.52. “userget” Command

This command is used to check all users’ accounts and rights except passwords which are hidden.

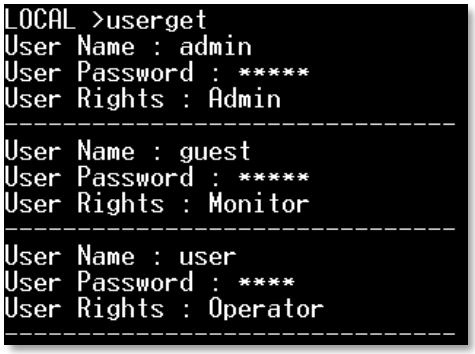


Figure 6-58 “userget” Command

25.53. “uiget” Command

This command is used to check all user interfaces.

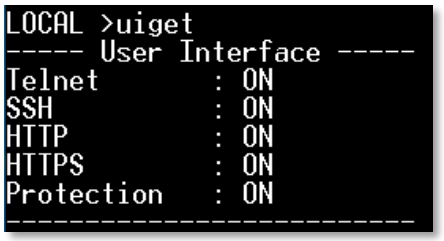


Figure 6-59 “uiget” Command

25.54. “uiset” Command

This command is used to set a range of IP addresses to permit or limit user interfaces operation, such as Telnet, SSH, HTTP and HTTPS. Also, account protection is enabled or disabled by this command to prevent brute-force attacks.

```
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

25.55. “vipget” Command

This command is used to check “**Virtual IP**” in routing mode.

```
LOCAL >vipg

---------- CLI_VIP_GET_Help ----------------
 Usage   : Get Virtual IP Settings
 Synopsis:
    vipget [Options]
 ==========================================

 Options:
    -a          Show ALL Settings on VIPs
    -i          Show IP table only

LOCAL >vipg -a
---------- Virtual IP Table ----------------------------------------------------
Ind | Interface | Mode | IP | Mask | Gw(ON*) | Desired | Name | VPN | IF Srvs
==============================================================================

  1 | eth0.1    |Static| 192.168.10.25   | 255.255.255.0   | *192.168.10.254
                |Static| 0.0.0.0         | 0.0.0.0         |
                 Desired Service  |
                 Name             | admin
                 VPN Server IP    | 192.168.0.254
                 DHCP service     |   ON
                 DNS service      |   ON
                 ROUTE service    |   ON
------------------------------------------------------------------------------
```

Figure 6-61 “vipget” Command

25.56. “vipset” Command

This 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

25.57. “vrget” Command

This command is used to check routing rules in the 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

25.58. “vrset” Command

This command is used to set routing rules. One of the main functions is named “Static Route”, and rules can be manually added or deleted. RIPv1 & RIPv2 are also configurable.

```
LOCAL >vrset
Incomplete format.

---------- CLI_VR_SET_Help ---------------
 Usage   : Set Routing Rules
 Synopsis:
    vrset [-m]/[-d -i -n -g -v]
 ============================================
 Options:
   Dynamic :
     -m      [0~2]   set Dynamic Routing Mode  0:Off, 1:RIPv1, 2:RIPv2
   Static :
     -d     [1~30]   Delete rule x
     -i     [IPv4]   Destination domain
     -n     [IPv4]   Netmask
     -g     [IPv4]   Gateway
     -v     [1~4094] VLAN Tag
 Example:
     1. Set Dynamic Routing Mode : RIPv2
        vrset -m 2
     2. add static rule
        vrset -i 172.15.0.0 -n 255.255.0.0 -g 172.16.0.254 -v 1
     3. delete static rule
        vrset -d 1
```

Figure 6-64 “vrset” Command

25.59. “vrrpget” Command

This command is used to get VRRP Information.

```
LOCAL >vrrpg
                    VRRP Configuration
 Interface | Entry | Admin | State    | ID  | Pri / Track | IP
-----------+-------+-------+----------+-----+-------------+---------
 eth0.1    | 1     | OFF   | —        |   1 | 100 / ETH1  | 0.0.0.0
           | 2     | OFF   | —        |   1 | 100 / ETH1  | 0.0.0.0
```

Figure 6-65 “vrrpget” Command

25.60. “vrrpset” Command

This command is used to set VRRP parameters, such as Interface VLAN, Priority, and VRRP IP.

```
LOCAL >vrrps

---------- 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]    ETH1 ~ ETH4
          [5]      MLP
 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 ETH1
     vrrps -v 1 -t 1
```

Figure 6-66 “vrrpset” Command

25.61. “lfpget” Command

This command is used to Link Fault Pass through Information.

```
Local >help lfpget

------- CLI Link Fault Pass Through Help ------
 Usage   : Get Link Fault Pass Through Status
 Synopsis:
    lfpget [Options]
 ============================================
 Options:
    -m          Show Link Fault Pass Through Mode
    -l          Show Link Fault Carry Forward Status

Local >lfpget
Link Fault Pass Through Mode : OFF
---------------- LLCF ----------------------------------------------------
 Port  |  LLCF | Link State | LAN-1 | LAN-2 | LAN-3 | LAN-4 |  DSL
--------------------------------------------------------------------------
 LAN-1 |  OFF  | Link Up    |   -   |   X   |   X   |   X   |   X
 LAN-2 |  OFF  | Link Up    |   X   |   -   |   X   |   X   |   X
 LAN-3 |  OFF  | Link Up    |   X   |   X   |   -   |   X   |   X
 LAN-4 |  OFF  | Link Down  |   X   |   X   |   X   |   -   |   X
  DSL  |  OFF  | Link Down  |   X   |   X   |   X   |   X   |   -
```

Figure 6-67 “lfpget” Command

25.62. “lfpset” Command

This command is used to setup Link Fault Pass through for VRRP members. This may help to setup “Link Fault” status for all interfaces in same group.

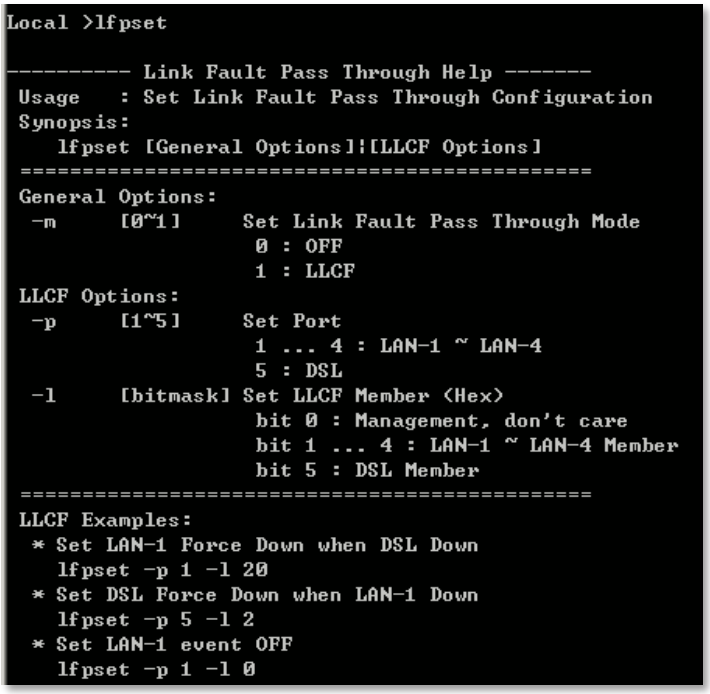


Figure 6-68 "lfpset" Command

Pin Assignment

A.1 Console Pin Assignment

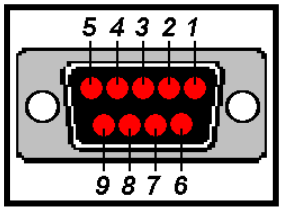


Figure A-1 DB-9 Interface

The Console DB-9 pin assignment is as follows:

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

Table A-1 DB-9 pin assignment

A.2 MLP RJ-45 Pin Assignment

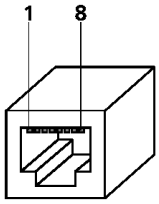


Figure A-2 DSL RJ-45 Pin Assignment

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)		

Table A-2 MLP RJ-45 pin assignment

A.3 ETH RJ-45 Pin Assignment

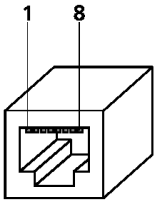


Figure A-3 LAN RJ-45 Pin Assignment

Table A-3 ETH RJ-45 pin assignment

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

A.4 ML630R DIP switches

Figure A-4 DIP switches

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

When both of DIP switches are set to “OFF” and then the ML630R is powered up, the ML630R will load the user’s latest profile which has previously been saved in the system. By default, the ML630R acts in **CPE** mode with IP address 192.168.0.1. When operators change and save the configuration, the modem will load the new boot profile for the next power on.

If only **DIP1** switch is set to “ON”, and then the ML630R is powered on, the ML630R will load the **CO**’s factory profile, and use the IP address that was previously configured. If the operator performed some configuration changes and saved them to the user’s profile, the system will also save the new configuration.

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