

MA4000-PX

**Operations and Maintenance Manual,
SW version 3.26.0**

Subscriber access/aggregation node

Document version	Date of issue	Content of revisions
Version 1.3		<p>Changed chapters:</p> <ul style="list-style-type: none">5.2 GPON PLC8 Interface Module11.2 User List Preview11.8 User Authentication Configuration23 MULTICAST configuration24 DHCP Relay Agent configuration25 PPPOE INTERMEDIATE AGENT configuration <p>Added chapters:</p> <ul style="list-style-type: none">12.6 Radius configuration23.3 Pv6 Multicast configuration24.4 DHCPv6 Relay Agent profiles management24.5 DHCPv6 Relay Agent profiles configuration26 IP Source Guard configuration28.5 Tunnelling configuration36 ONT Licensing
Version 1.2	25.04.2016	Commands for SW version 3.24.3
Version 1.1	26.02.2016	Commands for SW version 3.24.1
Version 1.0	02.06.2015	First publication.
Software version	3.26.0	

TABLE OF CONTENTS

TABLE OF CONTENTS	3
PART I GENERAL	9
1 INTRODUCTION	10
2 ARTICLE DESCRIPTION	11
2.1 Purpose	11
2.2 Application variants	12
3 DELIVERY SET	13
4 HARDWARE CONFIGURATION FOR MA4000-PX ACCESS NODE.....	14
4.1 Crate	14
4.2 PP4X Central Switch Module.....	18
4.3 GPON PLC8 Interface Module	21
5 MA4000-PX ARCHITECTURE	24
5.1 PP4X Central Switch Module.....	25
5.2 GPON PLC8 Interface Module	27
6 INSTALLATION AND CONNECTION	28
6.1 General Requirements	28
6.2 Equipment Installation	30
6.2.1 Preparations for Installation	30
6.2.2 Device Arrangement and Mounting Requirements.....	30
6.2.3 Rack Mount Installation of the Device	31
6.2.4 Laying and Connecting Cables.....	32
PART II GETTING STARTED WITH THE ACCESS NODE	34
7 CONNECTING ACCESS NODE TO CLI	35
7.1 Introduction	35
7.2 Connecting to CLI via COM Port.....	35
7.3 Connecting to CLI with Telnet Protocol	36
7.4 Connecting to CLI with Secure Shell Protocol	38
8 GETTING STARTED WITH THE ACCESS NODE CLI.....	39
8.1 Introduction	39
8.2 Command line operation principles.....	39
8.3 Command System Structure	40
PART III ACCESS NODE CONFIGURATION	43
9 ACCESS NODE CONFIGURATION	44
9.1 Configuration Structure	44
9.1.1 Introduction	44
9.1.2 Configuration Structure	44
9.2 Lifecycle of Configuration	44
9.3 Creating Configuration Backup	45
9.4 Configuration Restore	46
9.5 Configuration Reset	46
10 NETWORK SETTINGS.....	47
10.1 Introduction	47
10.2 Adjustment of Network Settings.....	47
11 USER MANAGEMENT.....	48
11.1 Introduction	48
11.2 User List Preview.....	49
11.3 Adding a New User.....	49
11.4 Changing User Password.....	49
11.5 Viewing and Changing User Access Rights.....	50
11.6 Deleting a User.....	50

11.7 User Session Configuration	50
11.8 User Authentication Configuration	51
12 SERVICE CONFIGURATION	52
12.1 SNMP Configuration.....	52
12.2 System Log Configuration	52
12.3 SSH Configuration	53
12.4 Telnet Configuration	53
12.5 Tacacs/Tacacs+ Configuration.....	54
12.6 Radius configuration	54
12.7 Sntp Configuration	55
13 VLAN CONFIGURATION	56
13.1 Introduction	56
13.2 Adding a VLAN.....	56
13.3 VLAN Configuration.....	56
13.4 Deleting a VLAN.....	57
14 PP4X STACKING CONFIGURATION	58
15 INTERFACES CONFIGURATION.....	59
15.1 Introduction	59
15.2 Ethernet Interfaces Configuration	60
15.3 GPON Interfaces Configuration.....	61
16 ISOLATION GROUP CONFIGURATION	62
16.1 Introduction	62
16.2 Isolation Group Configuration.....	62
17 SELECTIVE Q-IN-Q CONFIGURATION	64
17.1 Introduction	64
17.2 Selective Q-in-Q Configuration	64
18 QOS CONFIGURATION	65
19 LAG CONFIGURATION.....	66
19.1 Introduction	66
19.2 LAG Configuration	67
20 SPANNING TREE CONFIGURATION	69
20.1 Introduction	69
20.2 Spanning Tree Configuration.....	69
21 DUAL HOMING CONFIGURATION.....	71
21.1 Introduction	71
21.2 Dual Homing Configuration.....	71
22 LLDP CONFIGURATION	72
22.1 Introduction	72
22.2 LLDP Configuration.....	72
23 MULTICAST CONFIGURATION	73
23.1 Introduction	73
23.2 Multicast Configuration	74
23.3 IPv6 Multicast Configuration.....	75
24 DHCP RELAY AGENT CONFIGURATION	77
24.1 Introduction	77
24.2 DHCP Relay Agent Profiles Management.....	79
24.3 DHCP Relay Agent Profiles Configuration	80
24.4 DHCPv6 Relay Agent profiles management	81
24.5 DHCPv6 Relay Agent profiles configuration.....	81
24.6 DHCP Broadcast-to-Unicast Relay Agent Configuration	82
25 PPPOE INTERMEDIATE AGENT CONFIGURATION.....	83
25.1 Introduction	83
25.2 PPPoE Intermediate Agent Profiles Configuration.....	83

26 IP SOURCE GUARD CONFIGURATION	85
26.1 Introduction	85
26.2 IP Source Guard configuration	85
PART IV ONT CONFIGURATION	87
27 SERVICE MODELS.....	88
27.1 Introduction	88
27.1.1 "VLAN for Subscriber" Architecture.....	88
27.1.2 "VLAN for Service" Architecture	89
27.2 Operating Principle	89
27.2.1 Model 1	90
27.2.2 Model 2	91
27.2.3 Model 3	91
27.3 Model Configuration	92
28 ONT CONFIGURATION	94
28.1 Introduction	94
28.2 General Configuration Principles	94
28.3 ONT Profiles Configuration	96
28.3.1 Cross-Connect Profile Configuration.....	96
28.3.2 DBA Profile Configuration	96
28.3.3 Shaper Profile Configuration.....	96
28.3.4 Ports Profile Configuration	97
28.3.5 Management Profile Configuration	97
28.4 ONT Configuration Procedure.....	98
28.4.1 Model 1	100
28.4.2 Model 2	104
28.4.3 Model 3	104
28.5 Tunnelling configuration	107
29 DBA CONFIGURATION	111
29.1 Introduction	111
29.2 DBA Profiles Assignment.....	113
29.2.1 Services in Different T-CONTs	113
29.2.2 Services in One T-CONT	114
29.2.3 One Profile for Multiple ONTs.....	114
29.2.4 Profiles Assignment Example	115
29.3 DBA Configuration.....	116
29.3.1 T-CONT Type 1 Configuration	116
29.3.2 T-CONT Type 2 Configuration	117
29.3.3 T-CONT Type 3 Configuration	118
29.3.4 T-CONT Type 4 Configuration	118
29.3.5 T-CONT Type 5 Configuration	119
30 RG ONT CONFIGURATION	121
30.1 Introduction	121
30.2 Services Combined Configuration.....	122
31 HIGH SPEED INTERNET CONFIGURATION.....	125
32 MULTICAST CONFIGURATION	126
32.1 Introduction	126
32.2 Model 1 Multicast Configuration	126
32.3 Model 2 (3) Multicast Configuration.....	129
33 VOIP CONFIGURATION	132
33.1 Introduction	132
33.2 VoIP Configuration in OMCI Management Domain	132
33.3 VoIP Configuration in RG Management Domain	133
34 TR-069 PROTOCOL MANAGEMENT CONFIGURATION	134

34.1 Introduction	134
34.2 Configuration of a TR-069 Inband management channel	134
34.3 Configuration of a TR-069 OOB Management Channel	135
34.4 TR-069 Client Configuration	136
35 ONT CONFIGURATIONS TEMPLATES	138
35.1 Introduction	138
35.2 ONT Configuration Templates.....	138
35.3 ONT Configuration Templates Assignment	138
35.4 ONT Configuration Preview with Templates.....	139
36 ONT LICENSING.....	140
36.1 Introduction	140
36.2 Loading a License File to OLT	140
PART V ACCESS NODE MONITORING	142
37 GENERAL INFORMATION	143
37.1 View Current SW Version of Access Node	143
37.2 View Information on Access Node	143
37.3 Interface Module Status View.....	144
37.4 Access Node Uptime View	144
37.5 Network Connection Check.....	144
38 ACCESS NODE RUN-TIME LOG	145
39 ACTIVE ALARMS LOG	146
39.1 Introduction	146
39.2 Alarm Generation and Registration	146
39.2.1 Structure of Alarm/Event	146
39.2.2 Alarm rates.....	146
39.2.3 Alarms	147
39.2.4 Normalization of Alarms	148
39.2.5 Reports	149
40 PP4X MONITORING	151
40.1 PP4X Resource Status.....	151
40.2 MAC Address Table Preview	152
40.3 PP4X Interface Status Preview	153
40.4 PP4X Interface Statistics Preview	154
40.5 Interface Mirroring.....	155
40.5.1 Controlled Port Configuration.....	155
40.5.2 Controlling Port Configuration	155
41 PLC8 MONITORING.....	156
41.1 GPON OLT State	156
41.2 GPON Interface State	156
41.3 MAC Table Preview	157
41.4 Statistics for GPON Interfaces	158
41.5 Statistics for OLT V Interfaces	158
41.6 Multicast Statistics	159
42 ONT MONITORING.....	160
42.1 ONT Configurations List	160
42.2 Active ONT List	160
42.3 Online ONT List.....	160
42.4 Offline ONT List	161
42.5 ONT Statistics	161
42.6 ONT Bit Error Rate.....	162
PART VI MAINTENANCE.....	163
43 REPLACEMENT OF PWR IN POWER INPUT MODULES.....	164
44 REPLACEMENT OF MFC MODULE.....	165

45 REPLACEMENT OF PP4X CENTRAL SWITCH MODULES	166
46 REPLACEMENT OF PLC8 GPON INTERFACE MODULES.....	167
47 SFP TRANSCEIVERS REPLACEMENT	169
48 PP4X FIRMWARE UPDATE	170
48.1 Firmware Update via CLI	170
48.1.1 Introduction	170
48.1.2 New firmware version installation procedure	170
48.1.3 Examples of the new firmware version installation procedure.....	172
48.2 Firmware Update via Bootloader (U-Boot).....	173
48.2.1 Firmware Update via Bootloader.....	173
48.2.2 Possible Abnormal Situations During the Firmware Upgrade via Bootloader.....	175
49 EMERGENCY RECOVERY OF PP4X FIRMWARE	176
50 ONT FIRMWARE UPDATE	177
50.1 Introduction	177
50.2 Overview	177
50.3 ONT Firmware Files Management	178
50.4 ONT Firmware Manual Update.....	179
50.5 Configuration of ONT Firmware Auto Update.....	179
50.5.1 ONT Auto Update Modes.....	179
50.5.2 ONT Auto Update Rules	179
TECHNICAL SUPPORT	181

TERMS AND DEFINITIONS.

- **IGMP (*Internet Group Management Protocol*)** – network protocol used by nodes in a network which is based on IPv4 protocol to report the membership in IP-group to a network router as well as to perform other functions as to controlling the group routing.
- **IGMP snooping function** is used in multicast networks so that the working stations do not receive the multicast traffic without request.
- **IPv6 (*Internet Protocol version 6*)** – the latest version of the IP-protocol with the latter belonging to the network level of TCP/IP protocol stack. The IP protocol joins the network segments into a joint network providing delivery of data between any network nodes. IPv6 uses a 128-bit address (32 bits in IPv4).
- **LACP – (*link aggregation control protocol*)** – this protocol helps connect several physical ports together for shaping a separate logical channel.
- **MAC-address (*Media Access Control*)** – is a unique identifier comparable with the device physical interface.
- **VLAN (*Virtual Local Area Network*)** – virtual local area network. VLANs can make a part of a big LAN featuring certain rules of interaction with the other VLANs, or can be fully isolated from them.
- **Crate** – a structural element for installing modules in modular systems. It also performs a function of intermodule communication, power supply distribution and ventilation of modules.

Notes and Warnings



Notes comprise important information, advice or recommendations for using and setting the device.



Warnings inform a user on situations, which may harm a device or an individual, cause the device malfunction or data loss.

PART I

GENERAL

1 INTRODUCTION

MA4000-PX is a multifunctional modular node of subscriber access and aggregation. MA4000-PX is a new-generation device which incorporates various interfaces with a high density of ports for rendering broadband service access. GPON technology is used as the subscriber access technology. ETTH (FTTB) technology is used with the device operating in aggregation mode.

MA4000-PX subscriber access and aggregation node allows to create an economically profitable solution and may replace several GPON LTP-8X.

This Operations and Maintenance Manual details the purpose, basic technical characteristics, as well as configuring, monitoring and software replacement rules for MA4000-PX access node.

2 ARTICLE DESCRIPTION

2.1 Purpose

Multiservice access and aggregation node MA4000-PX is designed for building an access network based on GPON technology. The system enables to build a scalable, fault-resistant "last mile" network to ensure the highest safety standards, both in rural and in urban areas. The access node manages subscriber units, switching traffic and connections to the transport network.

The central element of the MA4000-PX is the scalable Ethernet switch level L2+ (PP4X), which works in cooperation with various types of interface modules. PLC8 optical access module is used to connect subscriber devices via GPON technology.

Key advantages of the modular architecture are as follows:

- a step-by-step network upgrade without interruptions;
- high capacity determined by an unblocked switching capacity of a node;
- handling basket modules as an integrated device.

2.2 Application variants

MA4000-PX functions as a subscriber access node. Connection with the subscriber devices is provided by the peripheral modules PLC8 featuring 8 PON ports, each of them allows connecting up to 64 subscribers. Traffic switching and connection with the transport network are ensured by PP4X central processor modules which are connected by the peripheral modules via common high-speed bus of the device. Connection with the higher level equipment is effected by means of 10G(SFP+) interfaces and 1G combined interfaces.

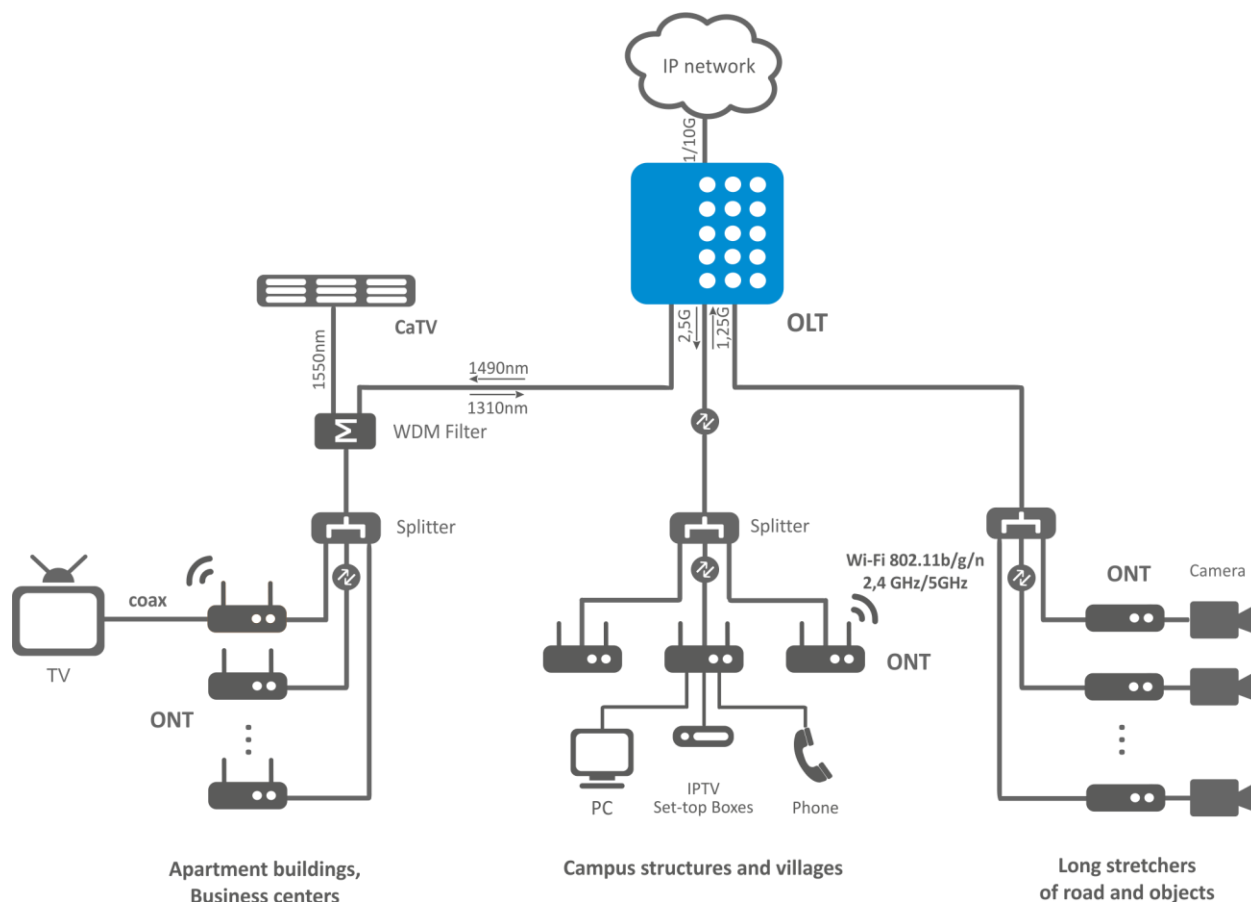


Fig. 1—MA4000-PX Subscriber Access/Aggregation Node Application Diagram

3 DELIVERY SET

The delivery set shall be determined by an equipment delivery contract.

A basic delivery set shall include:

- MA4000-PX equipment and SPTA set according to an order;
- Operations and Maintenance Manual;
- logbook;
- Declaration of Conformity.

In addition to MA4000-PX equipment, the delivery set may also include:

- connecting cable RS-232 DB9F – DB9F;
- power cable;
- connector DB-15M of an object communication interface;
- optical transceivers SFP 1Gb;
- optical transceivers SFP+ 10Gb.

4 HARDWARE CONFIGURATION FOR MA4000-PX ACCESS NODE

This section describes the embodiment of MA4000-PX: it demonstrates an exterior view of the front panel of PP4X Ethernet switch, PLC-8 interface module as well as side panels of a crate; it describes plug and socket units, LED indicators and controls.

4.1 Crate

MA4000-PX device is metal cased and consists of one 19" crate featuring 9U height. The crate serves for uniting modules of different functional purpose ensuring interaction of modules through high-speed 10 Gbps communication lines as well as for power distribution and supporting and monitoring temperature mode of the entire device.

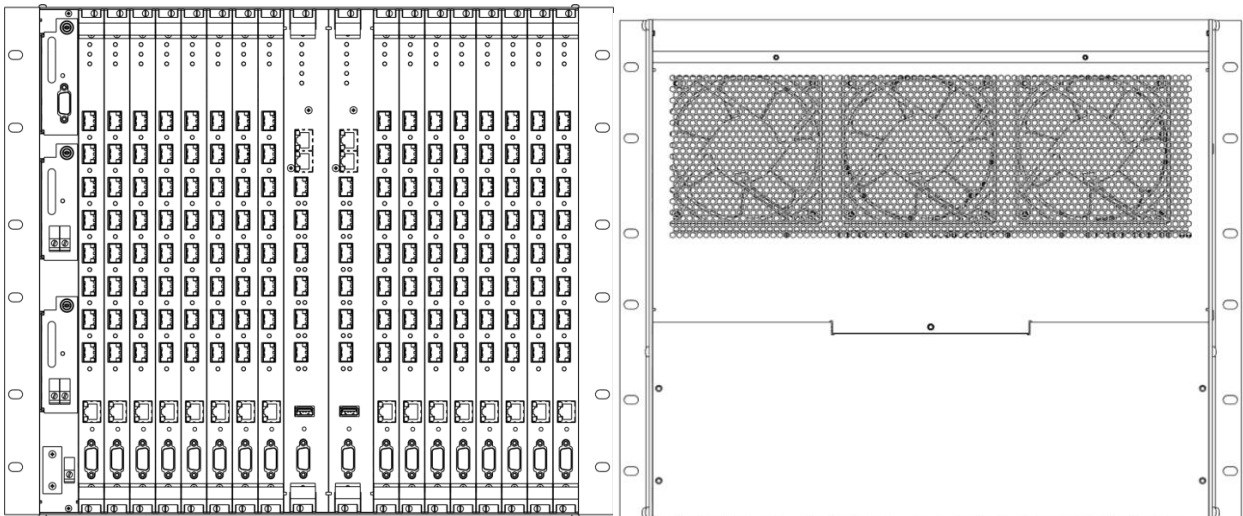


Fig. 2—Front and Rear External View of MA4000-PX Crate

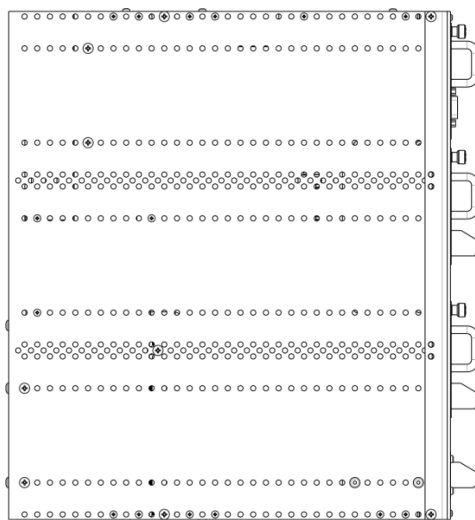


Fig. 3—Side View of MA4000-PX Crate

MA4000-PX's electric power supply system does not include group-type devices, which would determine reliability level of the entire system as a whole. The power supply is arranged by the distribution principle – every module has its own power unit. Herewith the crate functions only as a distributor of power to the modules.

The device has a front-to-rear ventilation system. Air flow diagram is shown in Figure 4.

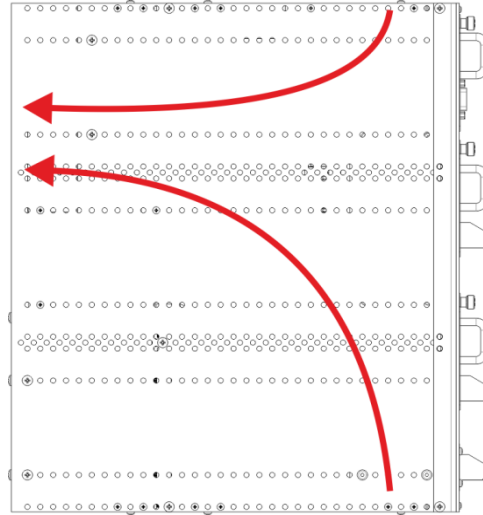


Fig. 4—Air Flow Diagram

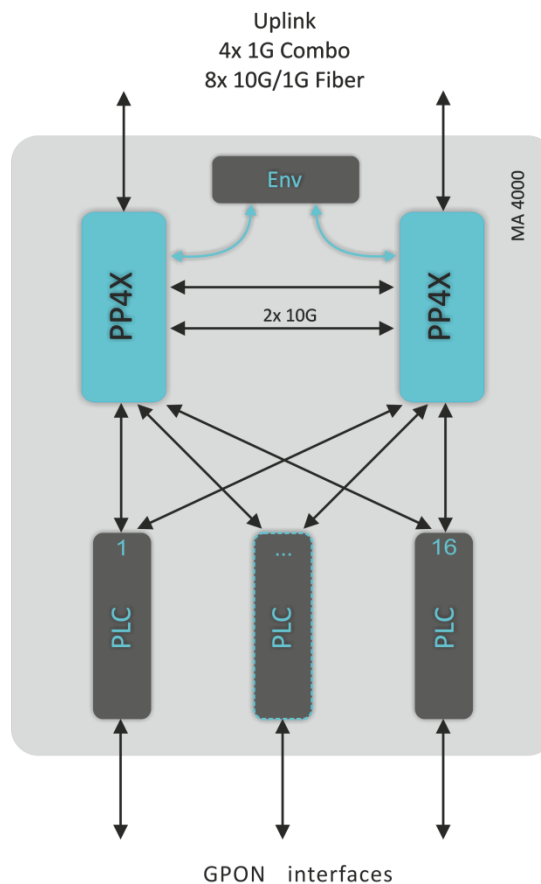


Fig. 5—Diagram of Modules Connections in a MA4000 Crate

The following designations are used in Figure 5:

- PLC – GPON interface module;
- PP4X – central switch module;
- Env – crate controller.

The crate composition depends on the application diagram. The crate features 18 positions for modules installation. PP4X central switch module is mandatory for installation into the crate. Up to two modules of this type can be installed for the sake of ensuring redundancy and increasing system productivity. Two central positions are intended for these modules installation (Ref. Figure 6).

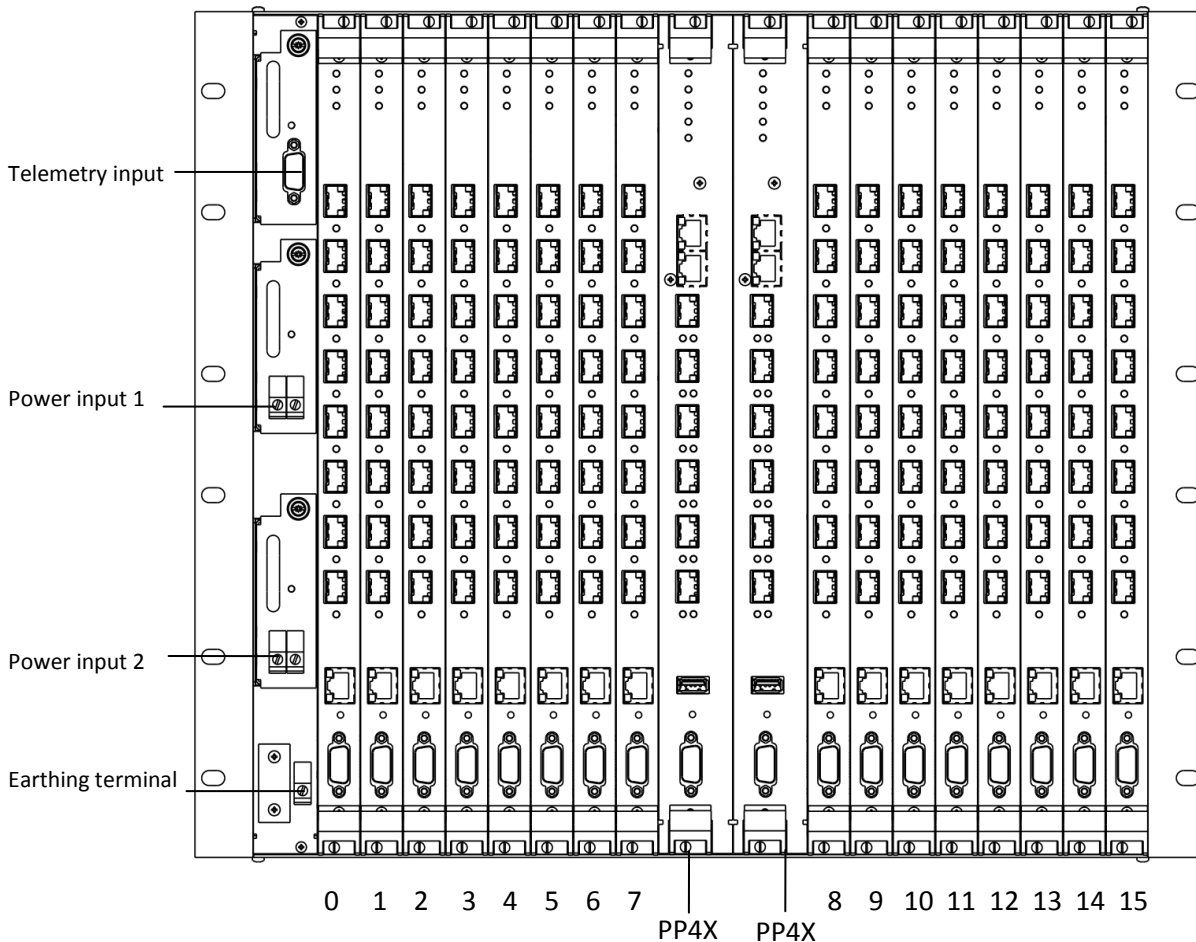


Fig. 6—MA4000-PX Crate Exterior

The other 16 positions in the crate are universal – any position may fit a PLC-8 interface module.

Installing the module PLC-8 is described in section [46 Replacement of PLC8 GPON interface modules](#).

In order to ensure interaction of modules, a module of cross-connections is installed in the crate. The module organizes interconnections between the central switches and interface modules. Every PP4X module features individual connection to every interface module and to the neighbour module PP4X. The intermodular connections correspond to the high-speed communication channels working at 10 Gbps speed. The system architecture shall be considered in detail in chapter 5.

The following elements are located in the left part of the crate:

1. Signalling connector. The connector is intended for communication with an object, where the equipment is installed, and can be used for connecting various-purpose sensors with “dry contacts” type interface as well for connecting different types of actuators.

2. Two power entry modules. In order to ensure the required level of reliability, the device is furnished with two power entries, which can be connected to two different power sources. The modules ensure automatic changeover to the standby power supply in case one of the supplies fails and protection from incorrect connection of the power supply feeders. The modules design allows to replace them in the course of device operation in case of alarm. The device provides for monitoring tools for power supply modules, i.e. input voltage and consumed current.

3. Earthing terminal.

Temperature control system of the device is designed to be used in combination with the air conditioning system of the equipment hall using hot and cold aisles principle. The ventilation system includes three fans arranged on the crate rear wall (Ref. Figure 2) and a controller to control the rotational speed of the fans. The fans controller module is installed inside the crate.

The ventilation system performance is adjustable and can vary within the limits of 7 m³/min to 14 m³/min. The acoustic noise level – not more than 36 dB(A).

Basic technical parameters of the access platform are given in Table 1.

Table 1—Basic technical parameters

General parameters	
Types of modules	PP4X – control and switching module PLC8 – 8 linear interfaces GPON 2.5 Gbps
Number of interface modules	Up to 16 modules
Bus type and performance	34x 10GBASE-KX (XAUI), 340 Gbps
Control	
Control interfaces	SNMP, CLI, Telnet, SSH
Physical characteristics and ambient conditions	
Supply voltage	36 .. 72 V
Consumed power	Not more than 850 W (at full load) ¹ ; Crate: not more than 35 W; PP4X: not more than 70 W; PLC8 without SFP ² : not more than 30 W; PLC8 with SFP ² : not more than 40 W; Fans: not more than 18 W.
Weight	Not more than 25 kg
Overall dimensions	480x400x350 mm
Temperature range	from -10 to +45°C
Humidity	Relative humidity – up to 80%
Average service life	20 years

¹ The maximum values for each of the elements have been considered when calculating the consumed power of a maximum loaded basket.

² Measurements have been made for PLC8 boards, version 2v0.

4.2 PP4X Central Switch Module

Central switch module is the main element of the platform, which generally manages and diagnoses peripheral modules, switching, aggregation and communication interface modules with higher level network equipment. The modules operate in the mode of load sharing and redundancy via two internal 10 Gbps interfaces.

The front panel external view, description of connectors, indicators and PP4X module controls are given in Figure 7.

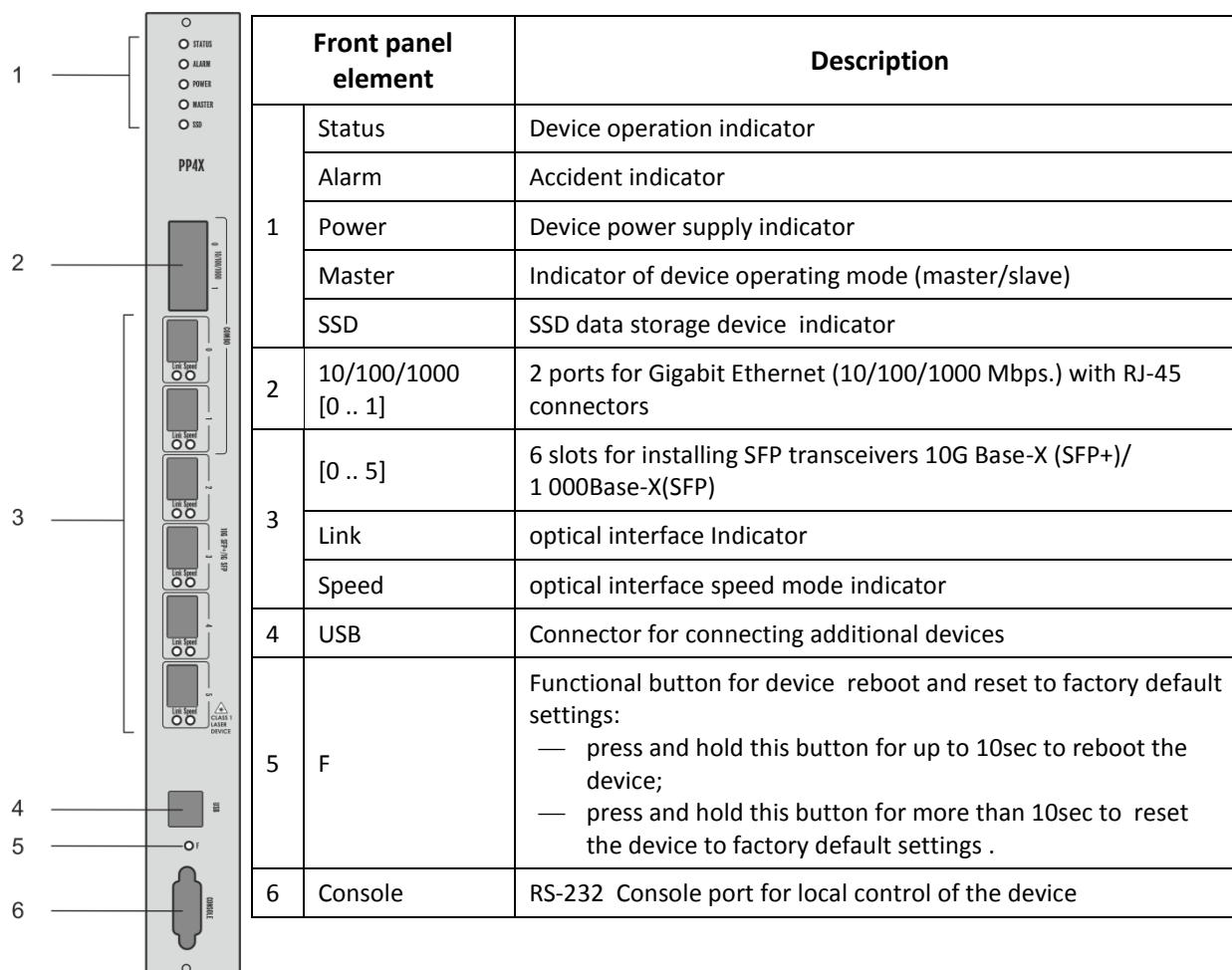


Fig. 7—Front panel external view, description of connectors, indicators and PP4X module controls



Two electrical Gigabit Ethernet interfaces with numbers 0, 1 and two optical interfaces with numbers 0, 1 are of a combined type. One interface only (electrical or optical), and not both of them simultaneously, can be active in combined ports.

Technical characteristics of the module are given in Table 2.

Table 2—PP4X module technical parameters

Processor	
Processor type	Marvell MV78x00, ARMv5TE architecture
Processor clock frequency	1000 MHz
Core quantity	2
Random-access memory	DDR2 SDRAM 512 MB 800 MHz
Non-volatile memory	1GB NAND Flash 2GB NAND Flash (since version 3v0)
Interfaces	
USB interface	Compatible with USB 2.0 specification
Network interfaces	External connections 4x10GBase-X(SFP+) 2x (10/100/1000Base-T/1000Base-X (SFP)) Inter-module connections 16x 10GXAUI (10GBASE-KX4)
Optical transceivers	1GSFP, 10G SFP+
Serial port	RS232, 115200 bit/s
Switch	
Ethernet switch	Marvell Packet Processor
Switch performance	480 Gbps
Table of MAC addresses	32K records
VLAN support	Up to 4K in accordance with 802.1Q
Quality of Service QoS	8 priority output queues for each port
Port quantity	24 ports up to 10 Gbps per port
Port modes	Duplex/half-duplex mode 10/100/1000 Mbps for electrical ports. Duplex mode 1/10 Gbps for optical ports.
Supported standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fibre Gigabit Ethernet ANSI/IEEE 802.3 NWayauto-negotiation IEEE 802.3x Full Duplex and flow control IEEE 802.3ad Link aggregation IEEE 802.1p Protocol for Traffic Prioritization IEEE 802.1Q Virtual LANs IEEE 802.1ad Provider Bridges (QinQ) IEEE 802.1v VLAN Classification by Protocol and Port IEEE 802.3 ac VLAN tagging IEEE 802.1d MAC bridges IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1s Multiple Spanning Trees IEEE 802.1x Port Based Network Access Control
Power consumption	Not more than 70 Watt

PP4X module current status is displayed by indicators **Status, Alarm, Power, Master, SSD, Link, Speed**. A list of indicator statuses and the values thereof are shown in the following tables:

Table 3—Module status light indicators

Indicator	Indicator status	Device status
Status	Green, continuously on	Normal operation
	Green, flashing at 1 sec intervals	Operation in a limited mode, F button was pressed when starting the device
	Red, on	The device is loading
Alarm	Off	No accidents
	Yellow, continuously on	Non-critical accident is available, one or more
	Red, continuously on	Critical module accident
Power	Green, continuously on	Module power supply is OK
	Red, continuously on	Failure of one or more module inner power supplies
	Off	Module power supply is not available
Master	Green, continuously on	The device operated as a master device in the crate
	Off	The device operated as a slave device
SSD	Green, on	Data storage carrier is connected
	Off	Carrier is not connected

Table 4—Combo-ports 0-1 status light indicators

Indicator	Indicator status	Device status
Link	Green, continuously on	Connection to an oncoming device is available
	Green, flashing	Data is being received or transmitted
	Off	Port is not connected
Speed	Yellow, continuously on	Connection at 1000 Mbps speed is established
	Off	If the Link indicator is on, it means that connection at speed 10 or 100 Mbps is established

Table 5—Ports 2-5 status light indicators

Indicator	Indicator status	Device status
10 Gbps mode		
Link	Green, continuously on	Connection to an oncoming device is available
	Green, flashing	Data transmission
Speed	Yellow, continuously on	Connection to an oncoming device at 10 Gbps speed is available
	Yellow, flashing	Data reception
Indication in 1Gbps mode		
Link	Green, continuously on	Connection to an oncoming device is available
	Green, flashing	Data exchange
Speed	Off	Connection to an oncoming device is being established at 1 Gbps speed

4.3 GPON PLC8 Interface Module

The PLC8 module is designed to organize broadband access to the data network via GPON technology at speeds of up to 2.5 Gbps in the direction to the user. This module is designed for use on the site of the "last mile" and enables to connect up to 512 communication terminals (ONT).

The front panel exterior view, description of connectors, indicators and controls for PLC8 module are shown in Figure 8.

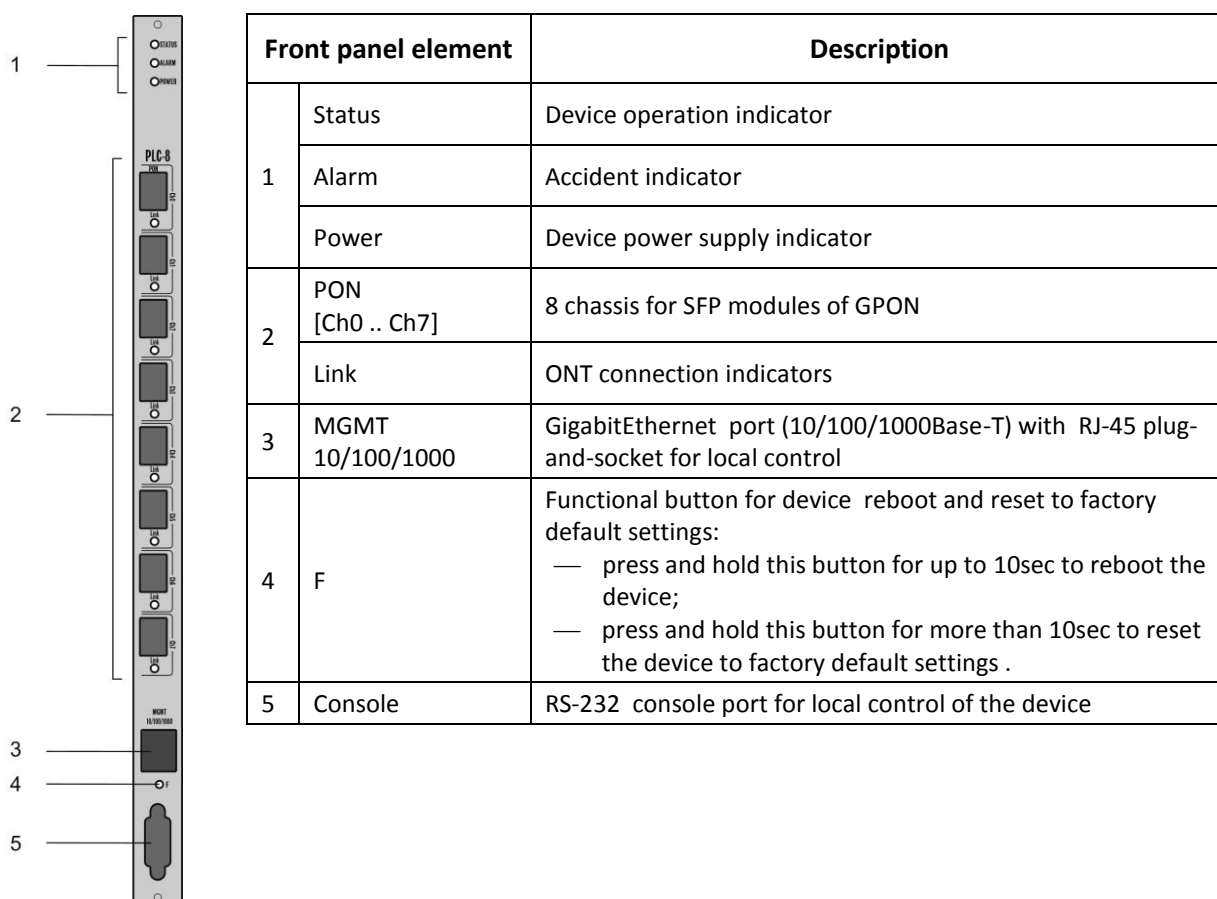


Fig. 8—Front panel exterior view, description of connectors, indicators and controls of PLC8 module

Table 6—Technical parameters for PLC8 module

Processor	
Processor type	Marvell Sheeva, ARMV5TE architecture
Processor clock frequency	800 MHz
Core quantity	1
Random-access memory	DDR2 SDRAM 256 MB 800 MHz
Non-volatile memory	32Mb Serial Flash
Interfaces	
Network interfaces	External connections 2x 10GXAUI (10GBASE-KX4)

	Inter-module connections 1x10/100/1000Base-T RJ45 – Management port 8x 2.5 GPON
Console port	RS232, 115200 bit/s
SFP PON parameters	
Connector type	SC/UPC
Receiver sensitivity	From -28 to -8 dB
Transmission medium	Single-mode fibre optical cable SMF 9/125, G.652
Optical power budget (up/downstream)	26 dB/24.5 dB
Minimal attenuation <i>upstream/downstream</i>	11 dB/15 dB
Optical emission spectral width <i>upstream/downstream</i> $\Delta\lambda$	1 nm/1 nm
Connection wavelength <i>upstream/downstream</i>	1310/1490 nm
Connection speed <i>upstream/downstream</i>	1.25/2.5 Gbps
Splitting ratio	1:4, 1:8, 1:16, 1:32, 1:64
Max. transmission distance	20 km
Switch	
Ethernet switch	MarvellPacketProcessor
Switch performance	128Gbps
Table of MAC addresses	16K records
VLAN support	Up to 4K in accordance with 802.1Q
Quality of Service QoS	8 output priority queues for each port
Port modes	Duplex/half duplex mode of 10/100/1000 Mbps Duplex mode of 10 Gbps for inter-module connections
Supported standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fibre Gigabit Ethernet ANSI/IEEE 802.3 NWayauto-negotiation IEEE 802.3x Full Duplex and flow control IEEE 802.3ad Link aggregation IEEE 802.1p Protocol for Traffic Prioritization IEEE 802.1Q Virtual LANs IEEE 802.1ad Provider Bridges (QinQ) IEEE 802.1v VLAN Classification by Protocol and Port IEEE 802.3 ac VLAN tagging IEEE 802.1d MAC bridges IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1s Multiple Spanning Trees IEEE 802.1x Port Based Network Access Control ITU-T G.984x
Power consumption	PLC8 without SFP ¹ : not more than 30 W; PLC8 with SFP ¹ : not more than 40 W.
Weight	not more than 2.5 kg.

¹ Measurements have been made for PLC8 boards, version 2v0.

The module current status of is displayed by indicators **Status**, **Alarm**, **Power**, **Link**. A list of indicator statuses is shown in Table 7.

Table 7—The device status light indicators

Indicator	Indicator status	Device status
Status	Green light on	Normal operation
	Red light on	The device is loading
Alarm	Off	Normal operation
	Flashing red light	Alarms, one or more
	Red light on	Error at program core loading
Power	Green light on	Device power supply is on
Link	Green light on	Connection with at least one ONT is established
	Red light on	Loss of communication with all ONT
	Off	Port is disabled

Correct and error-free operation of GPON interface requires exact parameters to be chosen and set for each transceiver type. This can be done only under laboratory conditions by the terminal vendor. Table 8 lists SFP transceivers for which seamless terminal operation is guaranteed.

DDMI (Digital Diagnostic Monitoring Interface) provides information about transceiver parameters such as temperature, power voltage, etc. DDMI also measures the level of ONT signal (RSSI). All compatible transceivers support this function.

Table 8—The List of Compatible SFP Transceivers

Vendor	SFP transceiver model	Class	DDMI
NEOPHOTONICS	PTB38J0-6538E-SC	B+	+
NEOPHOTONICS	38J0-6537E-STH1+	C+ HP	+
NEOPHOTONICS	38J0-6537E-STH2+	C+ HP	+
NEOPHOTONICS	38J0-6537E-STH3+	C+ HP	+
Ligent Photonics	LTE3680M-BC	B+	+
Ligent Photonics	LTE3680M-BH	B+	+
Ligent Photonics	LTE3680P-BC	C+	+
Ligent Photonics	LTE3680P-BH	C+	+
Ligent Photonics	LTE3680P-BC2	C+ HP	+
Fanghang	DLOLT43BCDS20	B+	+
Fanghang	DLOLT43CCDS20	C+	+
Fanghang	FH-DLT43CCDS20	C+	+

5 MA4000-PX ARCHITECTURE

MA4000-PX platform is a switching device for Ethernet networks with a distributed switching system. If combined with ONT subscriber devices, MA4000-PX data transmission networks (from its architecture perspective) perform functions relating to access and aggregation levels.

MA4000-PX logical structure is shown in Fig. 9.

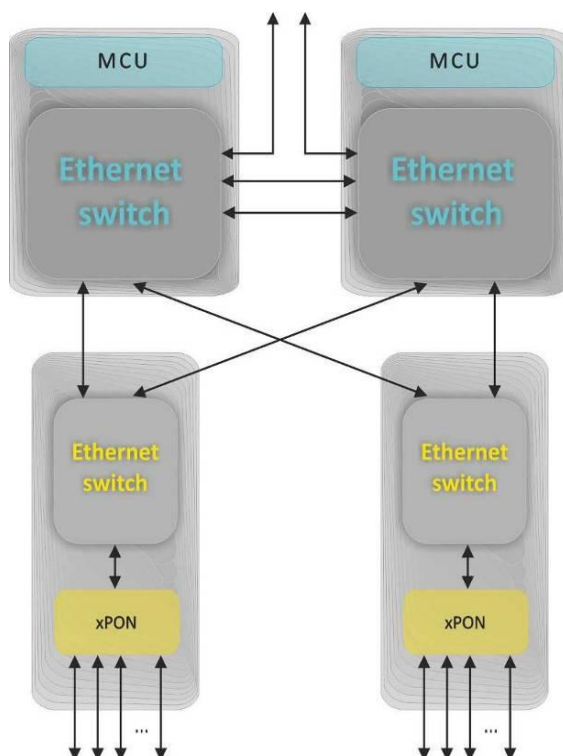


Fig. 9—MA4000-PX Access Platform Architecture

MA4000-PX is a two-level system of Ethernet switches.

The system centre has switches located on PP4X modules. They perform the aggregating function with respect to the modules of linear interfaces. The system may have one or two PP4X modules. The installation of two modules will help build a high-reliability system owing to the redundancy of switches and increase the system communications capacity due to distribution of data flows between the modules, the modules work in the stacking mode. PP4X modules stacking means there is a possibility to consolidate network interfaces, located at different modules, into trunk groups (LAG, LACP) and an integrated control interface.

The second system level: Ethernet switches located at modules of linear interfaces. These switches perform a function of aggregation with respect to the linear interfaces of a module, on which they are installed.

The interaction between modules occurs via 10Gbps connections. Each PP4X switch is connected to an interface module. Two PP4X are interconnected by two 10Gbps lines.

Access platform architecture is shown in Fig. 9.

5.1 PP4X Central Switch Module

Central switch module is the main element of the platform, which generally manages and diagnoses peripheral modules, switching, aggregation and communication interface modules with higher level network equipment. The modules operate in the mode of load sharing and redundancy via two internal 10 Gbps interfaces.

PP4X module block diagram is shown in Figure 10.

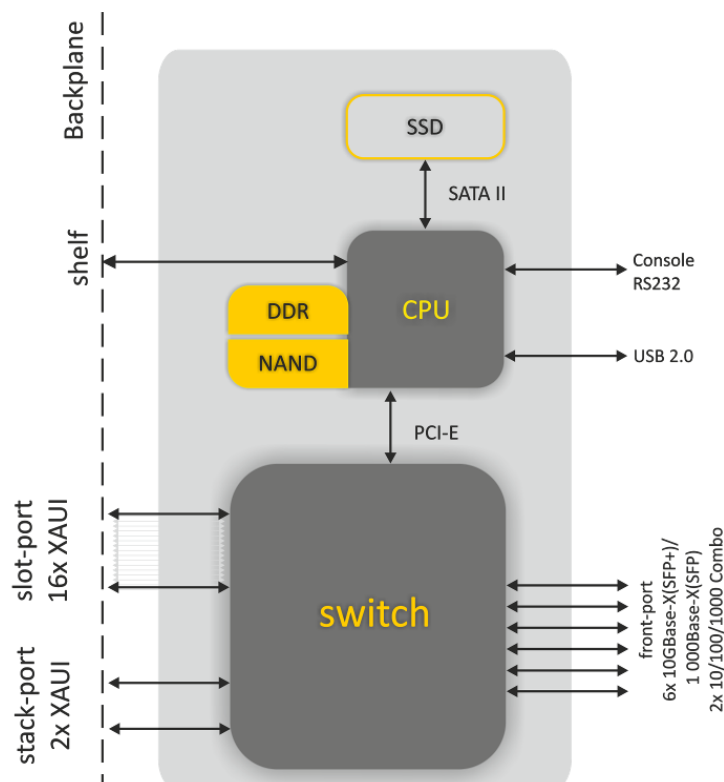


Fig. 10—PP4X Module block Diagram

The module comprises:

- *Processor core* incorporating CPU processor, random-access memory DDR, non-volatile memory NAND. The processor core controls local module resources, it also controls and monitors all modules incorporated into MA4000 device, stores and processes configuration data, controls and monitors the crate. Interaction between operator and processor core during control and monitoring procedures can be achieved via RS232 console or via network interface. The connection to Ethernet switch being a part of the module is used as the processor network interface. The processor has an interface, shown as 'shelf' in the Figure, to provide interaction with the crate controller. The USB interface is a universal one and can be used, e.g., for configuration data transferring and software update.
- *Ethernet switch* which ensures data transfer between devices and modules connected to its interfaces. The switch has 24 multimode ports which can operate at speed up to 12Gbps. The switch is controlled by a processor connected via PCI-Express interface.
- *Data storage device SSD* corresponds to a replaceable solid-state disk. Disks of different capacities may be used. SSD allows to store various-purpose data: configuration files of subscriber devices, system run-time journals, etc.

PP4X module features:

- Support for standard management interface through CLI, SNMP interfaces;
- Processing (changing, storing, archiving) configuration data for all device modules;
- Aggregate switch functions with the support of the following feature:
 - MAC address learning/aging;
 - MAC address quantity restriction;
 - Unknown MAC address processing;
 - Broadcasting traffic restriction;
 - Restricting multiaddress traffic;
 - Multiaddress traffic restriction;
 - Quantity of multicast group up to 2000;
 - Q-in-Q in accordance with IEEE802.1ad;
 - STP, RSTP, MSTP;
 - IGMP-proxy;
 - IGMP Snooping;
 - Fast switching between TV programs (IGMP fast leave);
 - Static routing¹;
 - Dynamic routing based on RIP, OSPF¹ protocols;
 - Bidirectional Forwarding Detect (BFD) for upstream interfaces¹;
 - Port isolation, Isolation of ports within one VLAN;
 - Static (LAG) and dynamic (LACP) aggregation of network interfaces, including interfaces belonging to different PP4X modules;
 - Data channels reservation with short recovery time (less than 1 sec) in case of failure.
- Interaction with external monitoring and control devices using Telnet, SSH, SNMP protocols;
- Collection of alarm data on interface modules and the entire device, forming accident and informational messages for monitoring systems;
- System run time journalizing and its storage in non-volatile memory;
- Device temperature and ventilation system control;
- Software update management for all modules of the device.

There is a restriction (shaper) for the management interface—500 packets per second. To ensure protection from ICMP flood, we have introduced additional restriction—40 ICMP packets per second.

¹ Not supported in this SW version

5.2 GPON PLC8 Interface Module

The purpose of PLC8 module is to shape the subscriber access transportation network based on GPON technology.

PLC8 module block diagram is shown in Figure 11.

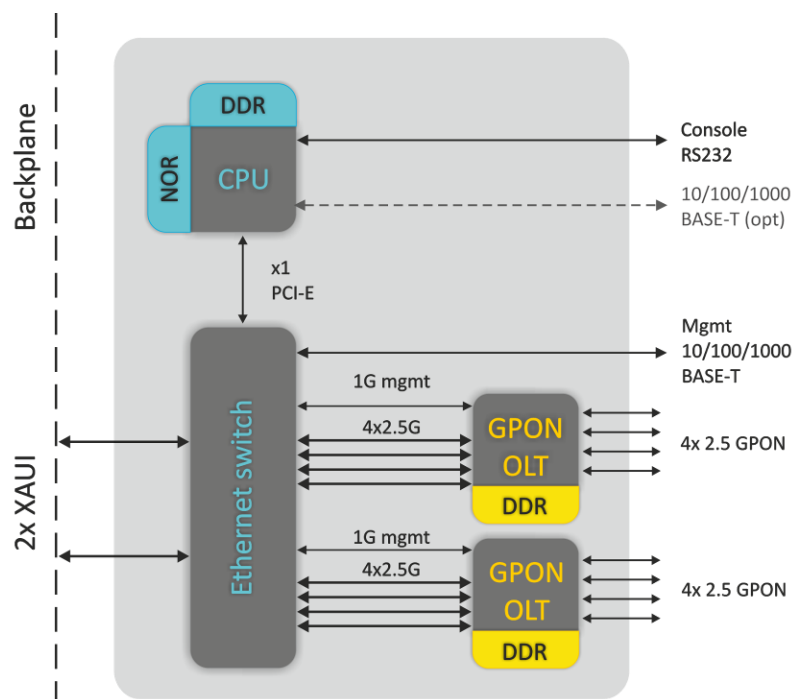


Fig. 11—PLC8 Module block Diagram

The module includes:

- Two four-channel batch-mode processors used as GPON OLT shape up eight GPON interfaces in accordance with ITU-TG.984. Up to 64 ONT or ONU devices can be connected to each interface via optical splitters;
- Packet Ethernet processor aggregating GPON transport flows and interacting via high-speed highway of MA4000-PX crate with central switches. In order to ensure device reliability and increase throughput capability, PLC8 module is provided with two interfaces interacting with central switches (uplink) – one for each of them. These interfaces work in aggregated channel mode (trunk or LAG). If MA4000-PX includes only one central switch, one of the interfaces is not used;
- Processor, which tasks include coordination and monitoring of packet processors operation, processing network protocols, supporting protocols for MA4000 device centralized control.

6 INSTALLATION AND CONNECTION

This Section provides safety instructions, procedures for equipment installation into a rack and connection to supply mains.

Prior to beginning the work it is necessary to carefully study working instructions and recommendations contained in equipment documentation.

Along with the safety requirements specified in this document and other documents accompanying the equipment, all industry relevant laws and regulations as well as operating company's individual requirements shall be observed when operating the equipment.

The personnel operating the equipment shall undergo relevant safety and operations training. Equipment may be handled by qualified personnel only.

In order to preclude personnel injuries and damage of equipment, all works shall be carried out in accordance with the following requirements.

6.1 General Requirements

Equipment installation:

- devices shall be installed in the premises, which help prevent unauthorized access to them;
- devices can be installed only above concrete or other surfaces that do not sustain combustion;
- prior to beginning operation the device shall be put steadily on a steady surface – on the floor or in a telecommunication cabinet;
- special attention to earthing shall be given during installation/deinstallation of the device. The earthing wire shall be primarily connected to the device during installation and disconnected last during deinstallation;
- for trouble-free operation of the equipment, a proper ventilation shall be ensured. There should be no foreign objects closer than 5 cm to ventilation openings available on equipment body;
- all the fasteners shall be tightened sufficiently after completing installation works.

Earthing:

- operating the device without correctly arranged earthing is not allowed. The earthing shall be arranged in accordance with Electrical Installations Code (EIC) requirements and shall be tested to comply with the Code requirements;
- a device or an equipment complex shall be connected to the protective earthing prior to operation (prior to connecting power supply feeders). The section of earthing conductors shall be not less than 10 mm²;
- in case additional instruments and devices are used together with the equipment which are powered from high-voltage mains, e.g., from 220 VAC mains, then such instruments shall be reliably earthed for protecting personnel and preserving equipment integrity.

Power supplies

- the device requires a DC power source;

- to connect power supplies, wires with sections corresponding to the maximum value of current used by a device shall be used;
- adherence to polarity is mandatory when connecting power feeders;
- available power supplies shall have protective devices to ensure quick load disconnection in case the maximum value for the device feed current had been exceeded;
- each power feeder shall be connected via a device which allows to promptly switch off – a circuit breaker or any other device;
- the device features two power inputs and can be connected to one or both power supplies. In order to switch off the device completely, it is necessary to disable all power supplies available.

Personnel safety

- no mounting or other works related to disconnection of cables from the device or disconnection of the device from the earthing circuits shall be performed during thunderstorm;
- to lift or move the device hold it by the crate elements. Do not load pushers by the basket weight at the front panels of modules and handles on the replacement in-feed modules and ventilation panel;
- two persons shall be engaged to move the basket;
- to protect eyes from laser radiation, do not peep into in the open optical ports. Infrared radiation of the lasers used in optical interfaces of devices can cause irreversible eye damage.

Qualifications of the personnel

- device installation, configuring and servicing shall be performed by qualified employees only;
- the device may be handle authorized personnel only ;
- any changes to the device (replacement of modules, software replacement) can be made by properly qualified and attested personnel;
- any alarms or failures in equipment operation shall immediately be reported to the on-duty personnel.

Prior to perform any types of works, all sections of documentation shall be carefully read.

6.2 Equipment Installation

6.2.1 Preparations for Installation

Prior to equipment installation ensure that mounting location requirements are met. No high temperatures, dust, harmful gases, combustible and explosive materials, sources of intensive electromagnetic radiation (radio stations, transformer substations, etc.), sources of loud sound shall be found at the places of equipment installation.

The installation place shall be compliant with the typical requirements to the places of telecommunication equipment installation.

If temperature in the premises without equipment exceeds 35°C, an air conditioner it shall be additionally installed. The air conditioner shall automatically start-up after blackouts. A stream of cooled air shall not blow right to the equipment, instead it shall be uniformly distributed within the premises.

The device ventilation is organized following a diagram shown in Figure 4.

The following conditions shall be met for proper operation of the ventilation system:

- distance between the lower and the upper panels of the crate and the closest neighbouring equipment shall be not less than 1U (44.45 mm);
- distance between the rear panel of the crate and the rear panel of the wall shall be not less than 200 mm;
- earthing shall be arranged in the installation premises, the power supply system shall correspond to equipment characteristics with respect to consumed power.

6.2.2 Device Arrangement and Mounting Requirements

The device is intended for installation in the telecommunication cabinet. For maintenance operations, a free access to the device from the front and the rear shall be provided.

Example for equipment layout is shown in Figure 12.

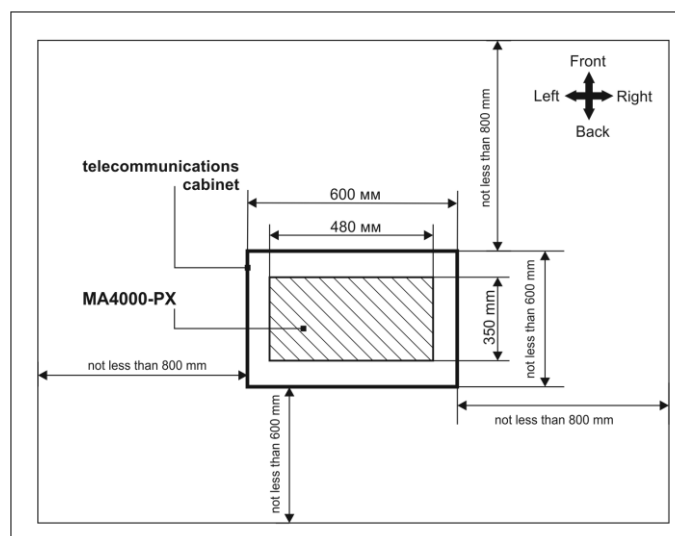


Fig. 12—Example for equipment layout in an equipment room

6.2.3 Rack Mount Installation of the Device

The crate of the device has attachment brackets intended for installation into telecommunication cabinet. The delivery set of the device includes fasteners.

The above ventilation requirements shall be met when arranging equipment in the cabinet. Figure 13 shows an example for device arrangement in the rack.

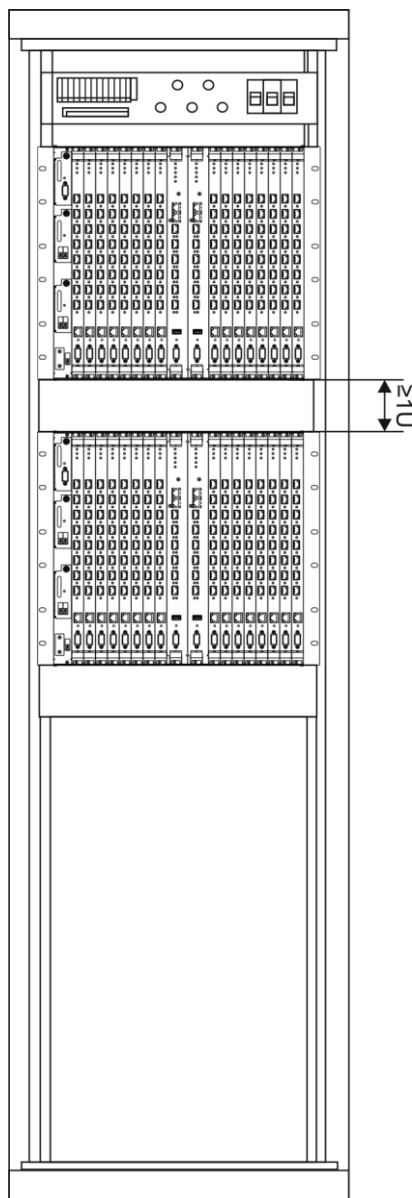


Fig. 13—Arrangement of MA4000-PX in a Rack

6.2.4 Laying and Connecting Cables

This Section explains an internal connections order to be made in the telecommunication cabinet.

Before connecting power feeders and communication lines to the device, earthing conductors shall be connected first.



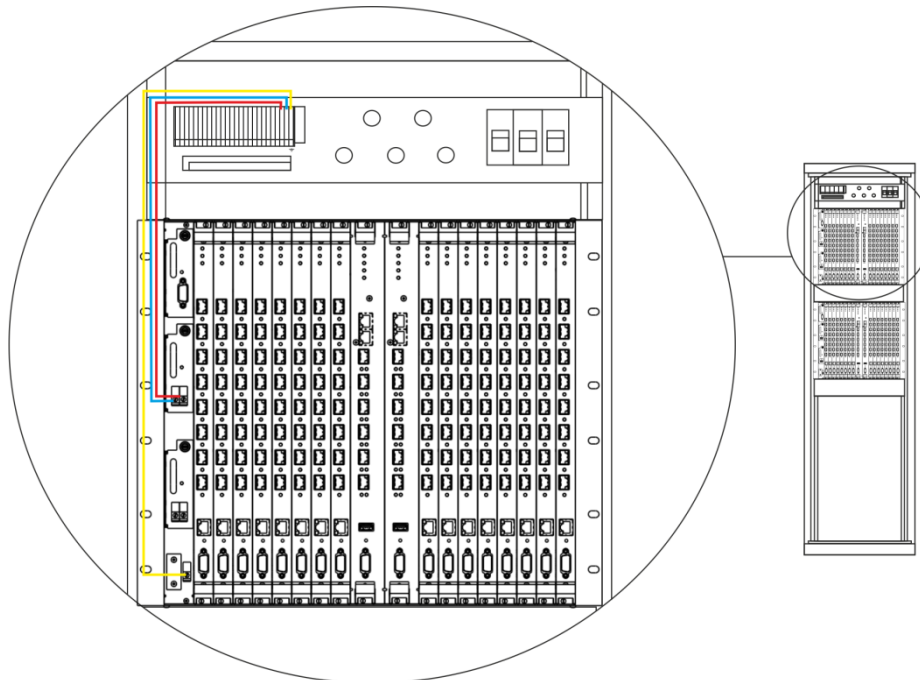
Telecommunication cabinet shall be earthed prior to perform works on feeding power to the devices.

At the next stage power cables shall be connected. One or two power feeders may be connected to the device. During connection works, adherence to polarity shall be ensures at all the stages.



All power sources shall be disabled when performing power connection works.

To supply power to the devices installed in the cabinet, a power distribution device shall be used. The equipment wiring diagram with a distribution device depends on its parameters. An approximate cable laying diagram is shown in Figure 14.




- Red – wire connecting device terminal “+” with positive power supply pole;
- Blue – wire connecting device terminal “-” with negative power supply pole;
- Yellow – earthing wire (earthing terminals at the device and earthing bar are marked with sign )

Fig. 14—Cable Laying and Connecting and Wire Earthing Diagram

The next stage involves connection of subscriber lines and data transmission lines. The lines shall be connected in accordance with the design diagram.

Data transmission lines shall be connected to the ports at PP4X control modules. An optical or copper wire can be used for connection works.

In case of laying optical cable outside the cabinet and leading it into the cabinet, measures shall be taken to protect the cable from damages by means of laying cable in the protective corrugated pipe. Cable bending radius when laying shall be not less than 40 mm. Cable organizers shall be used for horizontal cable laying in the equipment approach area.

In case of laying copper (electric cable) special attention shall be paid to protection of cable insulation and sheath from damage. The windows for cable feed-in into the cabinet shall be free from sharp cutting edges. In all cases laying of signal cables and data transmission cables in the same bundle with power cables shall be avoided.

PART II

GETTING STARTED WITH THE ACCESS NODE

7 CONNECTING ACCESS NODE TO CLI

7.1 Introduction

This Chapter describes various connection methods for Command Line Interface (CLI) of the access node.

A serial port (hereafter—COM port) is recommended for preliminary adjustment of the access node.

7.2 Connecting to CLI via COM Port

This type of connection requires PC either to have an integrated COM port or to be supplied with a USB-COM adapter cable. The PC should also have a terminal program installed, e.g. Hyperterminal.

Step 1. Using the null modem cable, connect the **CONSOLE** port of the PP4X master module ('Master' LED indicator should be solid green) to the COM port of the PC, see Fig. 15.

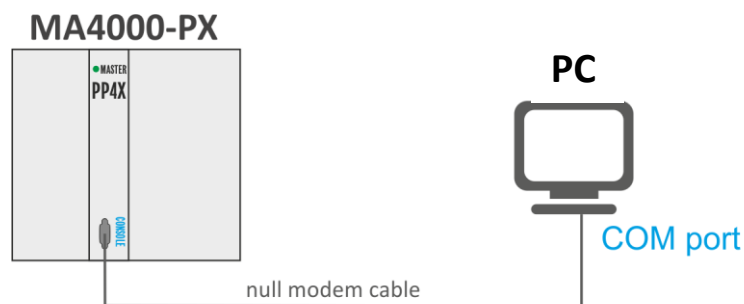


Fig. 15—Connecting access node to PC via COM port

Step 2. Launch the terminal program and create a new connection. Select the corresponding COM port in the "Connect to" drop-down list. Assign the port settings according to Table 9. Click OK.

Table 9—COM port parameters

Bit rate	115,200
Data bits	8
Parity	No
Stopping bits	1
Flow control	No

Step 3. Press **Enter**. Log into the device CLI.

Factory settings:

- login: **admin**
- password: **password**.

```
*****
*                               *
*      Welcome to MA4000      *
*                               *
*****

ma4000 login: admin
Password: *****

Technical support: http://eltex.nsk.ru/support
Wed Jan  8 11:58:08 T 2014

ma4000#
```

7.3 Connecting to CLI with Telnet Protocol

The Telnet protocol connection is more flexible than the connection via COM port. Connection to CLI can be established directly at the access node location or via IP network with the help of a remote desktop.

This section considers direct connection to CLI at the access node location. Remote connection is similar, but requires changes in the access node IP address which will be considered in details in Chapter *10 Network Settings*, page 47.

In order to be connected to the access node, a PC should have a NIC. The connection will additionally require the sufficient amount of network cable (Patching Cord RJ45) as it is not included in the delivery package.

Step 1. Connect the network cable to the **Gigabit Ethernet** port 0 or 1 (RJ-45 connector) of the PP4X master module ('Master' LED indicator should be solid green) and to the PC's network card, see Fig. 16.

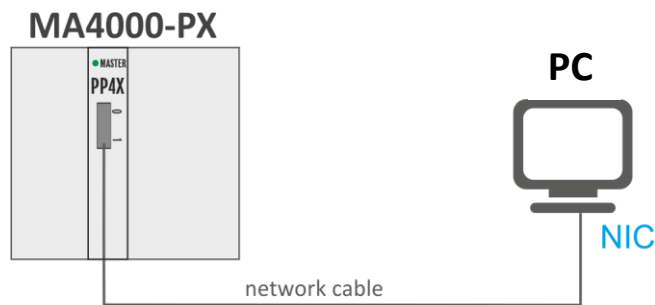


Fig. 16—Connecting access node to PC with the network cable

Step 2. Assign IP settings for the network connection:

- IP address: 192.168.1.1
- subnet mask: 255.255.255.0

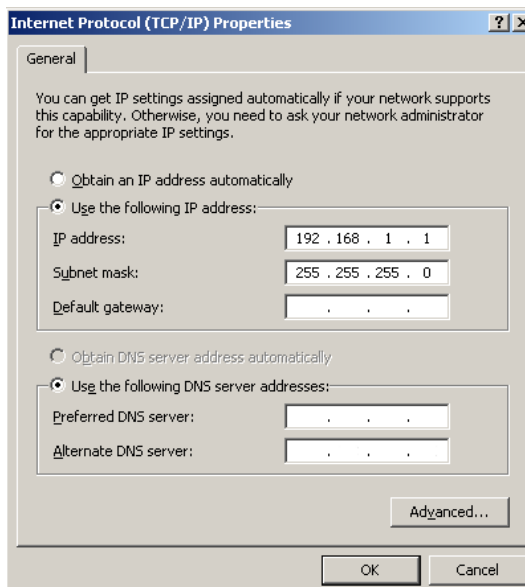


Fig. 17—Assigning network connection settings

Step 3. Click **Start -> Run**. Enter the **telnet** command and **IP address** of the access node. IP address factory setting: **192.168.1.2**. Click **OK**.

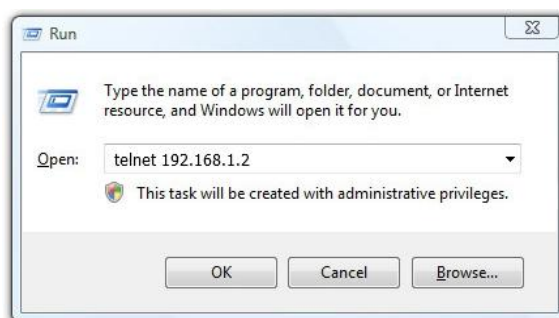


Fig. 18—Launching Telnet client

Step 4. Log into the terminal CLI.

Factory settings:

- login: **admin**
- password: **password**.

```
*****
*           Welcome to MA4000           *
*****

ma4000 login: admin
Password:

Technical support: http://eltex.nsk.ru/support
Mon Jan 13 13:40:02 T 2014

ma4000#
```

7.4 Connecting to CLI with Secure Shell Protocol

Secure Shell connection (SSH) has functionality similar to Telnet protocol. However, as opposed to Secure Shell, Telnet encrypts all traffic data, including passwords. This enables secure remote connection via public IP networks.

This section considers direct connection to CLI at the access node location. Remote connection is similar, but requires changes in the terminal IP address which will be considered in details in Chapter [10 Network Settings](#), page 47.

In order to be connected to the access node, a PC should have a NIC. The PC should have an SSH client installed, e.g. PuTTY. The connection will additionally require the sufficient amount of network cable (Patch Cord RJ45) as it is not included to the delivery package.

Step 1. Perform Steps 1 and 2 from Section [7.3 Connecting to CLI with Telnet Protocol](#).

Step 2. Run PuTTY. Enter IP address of the access node.

The factory setting for IP address is 192.168.1.2. Select port **22** and **SSH** protocol type. Click **Open**.

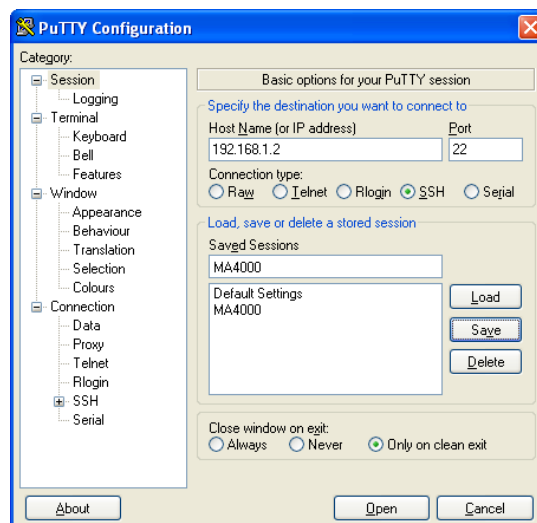


Fig. 19—Running SSH Client

Step 3. Log into the access node CLI.

Factory settings:

- login: **admin**
- password: **password**.

```
*****
*           Welcome to MA4000           *
*****

ma4000 login: admin
Password:

Technical support: http://eltex.nsk.ru/support
Mon Jan 13 13:40:02 T 2014
```

8 GETTING STARTED WITH THE ACCESS NODE CLI

8.1 Introduction

CLI is the main means of communication between user and the access node. This Chapter considers general operations in CLI.

Command Line Interface (CLI) allows to perform the device management and monitor its operation and status. You will require the PC application supporting Telnet protocol operation or direct connection via the console port (e.g. HyperTerminal).

8.2 Command line operation principles

To facilitate command line operation, the interface supports command autocompletion feature. To activate this feature, begin entering the command and enter <Tab> symbol.

Another feature, that simplifies the command line operation, is the context help. At this step you can get help on the following command elements by entering the question mark <?>.

For convenient device management via the command line, use do command, which allows to execute global layer commands (ROOT) from other layers of the command interface.

For instance:

```
ma4000# configure                                enter the device configuration mode
ma4000(config)# vlan 1
ma4000(vlan-1)# do show vlan 1
```

Vlans:		Tagged		Untagged	
VID	Name				
1	VLAN0001	slot-channel 0	(M)	front-port 1/0	(S)
		slot-channel 1	(M)	front-port 1/1	(S)
		slot-channel 2	(M)	front-port 1/2	(S)
...					
		plc-pon-port 0/7	(D)	-	
		plc-slot-channel 0/0	(D)	-	

Membership type: (S) - static, (D) - dynamic, (M) - slot-channels in management vlan

To make the work with commands easier, a hierarchical structure has been given to the entire system of commands. Use special transition commands to move between the hierarchy levels. It allows to use shorter commands for each level. To identify the level, where the user is currently located, the system prompt will change dynamically.

For instance:

```
ma4000# configure                                enter the device configuration mode
ma4000(config)#
ma4000(config)# exit                             return to the highest command system layer
ma4000#
```

To ease and simplify the work with the command line, we have implemented the hotkey support, see Table 10.

Table 10—CLI hotkey description

Hotkey	Description
Ctrl+D	In the nested section, return to the previous section ('exit' command); in the root section, exit the CLI ('logout' command).
Ctrl+Z ¹	Go to the root section
Ctrl+A	Go to the beginning of the line
Ctrl+E	Go to the end of the line
Ctrl+U	Delete characters to the left from the cursor
Ctrl+K	Delete characters to the right from the cursor
Ctrl+C	Clear the line
Ctrl+W	Delete the word
Ctrl+B ¹	Move the cursor one character back
Ctrl+F ¹	Move the cursor one character forward

Command line interface enables user authorization and restricts access to commands depending on their access level, provided by the administrator.

You can create as many users as you like, access rights will be assigned individually to each user.



Only one user 'admin' with the password 'password' specified in the factory configuration.

The system supports multi-user privileged access.

8.3 Command System Structure

MA4000 command line interface command system is divided into the hierarchical levels—modes (view).

From the global ROOT mode, you can enter the device parameters' configuration mode—**CONFIG** mode. Only users with the access level 15 are able to enter the configuration mode.

To go there from the global ROOT mode, execute the following commands:

```
ma4000# configure terminal
ma4000(config)#
```

¹ Not supported in the current firmware version.

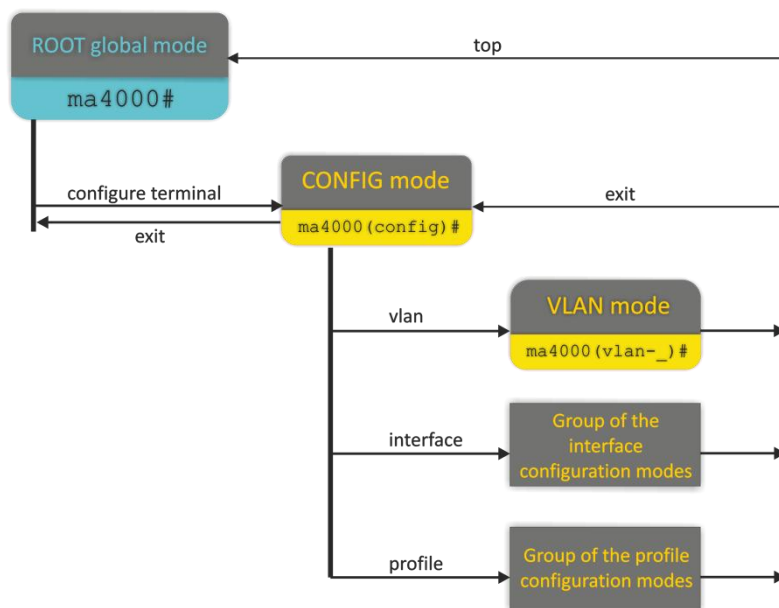


Fig. 20—Command mode hierarchy

The highest command hierarchy level is listed in the Table 11.

Table 11—Command mode hierarchy (the highest level)

Level	Entry command	Help string appearance	Previous level
Global mode (ROOT)		ma4000#	
MA4000 configuration management mode (CONFIG)	configure terminal	ma4000(config)#	ROOT
Interfaces Configuration	For detailed information, see Table 12		CONFIG
Profile configuration	For detailed information, see Table 13		CONFIG
VLAN configuration (VLAN)	vlan	ma4000(vlan-N)#	CONFIG

Table 12—Interface configuration command modes

Level	Entry command	Help string appearance	Previous level
PP4X module external uplink interface configuration (FRONT-PORT)	interface front-port	ma4000(front-port)#	CONFIG
Configuration of PLC8 module external GPON interfaces	interface gpon-port	ma4000(gpon-port)#	
GPON ONT configuration (PLC ONT)	ont	ma4000(config)(if-ont-0/0/0)#	
Configuration of PLC8 module external management interface (mgmt) (PLC FRONT-PORT)	interface plc-front-port	ma4000 (plc-front-port-x)#	
Configuration of management interfaces located between the Ethernet switch and PLC8 module olt chips (PLC MGMT-PON-PORT)	interface port plc-mgmt-pon-port	ma4000 (plc-mgmt-pon-port-x)#	

Configuration of PON interfaces located between the Ethernet switch and PLC8 module OLT chips (PLC PON-PORT)	interface plc-pon-port	ma4000 (plc-pon-port-x)#	
Configuration of the PLC8 module interface aggregation group used for connection to the PP4X module. (PLC SLOT-CHANNEL)	Interface plc-slot-channel	ma4000(plc-slot-channel-x)#	
Configuration of PLC8 module interfaces used for connection to PP4X. (PLC SLOT-PORT)	interface plc-slot-port	ma4000 (plc-slot-port-x)#	
LAG configuration of PP4X module uplink interfaces (PORT-CHANNEL)	interface port-channel	ma4000(port-channel-_)#	
LAG configuration of PP4X module interfaces for PLC8 modules (PORT-CHANNEL)	interface slot-channel	ma4000(slot-channel-_)#	
Configuration of PP4X module interfaces for PLC8 modules (SLOT-PORT)	interface slot-port	ma4000(slot-port-_)#	
Configuration of PP4X module internal stacking interfaces (STACK-PORT)	interface stack-port	ma4000(stack-port-_)#	

Table 13—Device profile command mode description

Level	Entry command	Help string appearance	Previous level
Address table profile configuration (PROFILE ADDRESS TABLE)	profile address_table	ma4000(config-address-table)("NAME")#	CONFIG
ONT GEM port profile configuration (PROFILE CROSS CONNECT)	profile cross-connect	ma4000(config-cross-connect)("NAME")#	
DBA profile configuration (PROFILE DBA)	profile dba	ma4000(config-dba)("NAME")#	
DHCP relay agent profile configuration (PROFILE DHCP_RA)	profile dhcp_ra	ma4000(config-dhcp-ra)("NAME")#	
ONT management profile configuration (PROFILE MANAGEMENT)	profile management profile management-by-name	ma4000(config-management)("NAME")#	
ONT port profile configuration (PROFILE PORTS)	profile ports	ma4000(config-ports)("NAME")#	
PPPoE intermediate agent profile configuration (PROFILE PPPoE_IA)	profile pppoe_ia	ma4000(config-pppoe-ia)("NAME")#	
Scripting profile configuration (PROFILE SCRIPTING)	profile scripting	ma4000(scripting)("NAME")#	
ONT bandwidth management profile configuration (PROFILE SHAPING)	profile shaping	(config-shaping)("NAME")#	
VLAN profile configuration (PROFILE VLAN)	profile vlan	ma4000(config-vlan)("NAME")#	

PART III

ACCESS NODE CONFIGURATION

9 ACCESS NODE CONFIGURATION

9.1 Configuration Structure

9.1.1 Introduction

A collection of all access node settings is referred to as configuration. This Chapter provides information about the parts configuration consists of. It also defines the lifecycle of configuration and describes main operations which can be performed.

9.1.2 Configuration Structure

The access node configuration can be arbitrarily divided into 3 parts. Fig. 21 shows the configuration structure.

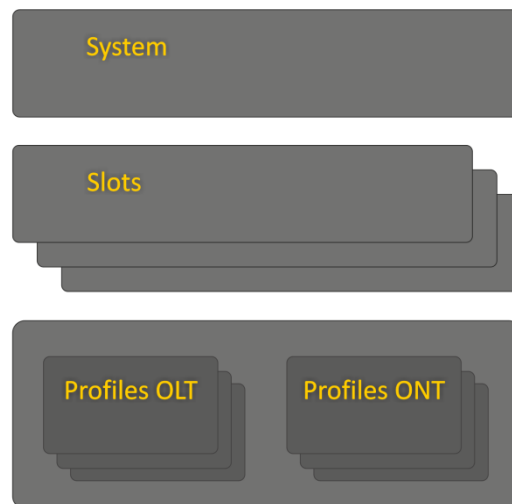


Fig. 21—Access node configuration structure

- *General system part.* This group includes such settings as network settings, services configuration, user table, etc.
- *SLOT—Slot configuration.* Contains PLC8 interface module settings.
- *Profiles—OLT and ONT profiles.* Contains OLT and ONT profile settings, that could be assigned to the PLC8 interface modules and ONT subscriber terminals respectively.

9.2 Lifecycle of Configuration

There are several configuration instances in the system:

- *Candidate*—a configuration under review.
- *Running*—an active configuration. It refers to the current configuration of the access node.
- *Backup*—keeps the previous active configuration; used when you need to roll back configuration changes.

Fig. 22 shows the diagram of configuration type changes.

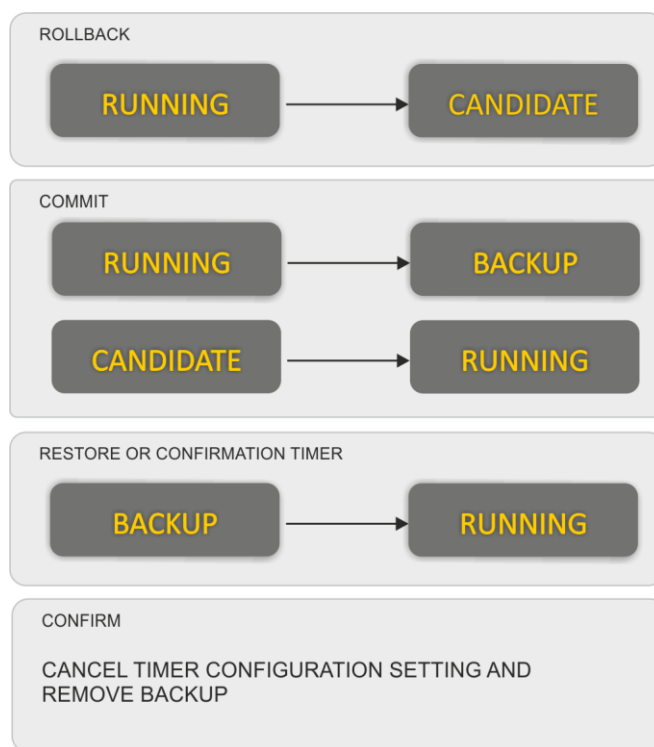


Fig. 22—Diagram of configuration type changes.

To apply changes made to the configuration, you should execute the **commit** command. After that, running configuration becomes backup configuration, and **RUNNING** is copied to **BACKUP**.

If you need to roll back configuration changes for some reason, perform the **rollback** operation. After that, the **CANDIDATE** configuration will be deleted. Next time configuration changes will be based on the **RUNNING** configuration.

To validate the applied configuration, the operator should enter the **confirm** command. If the confirmation is not provided until the expiration of the confirmation timer (default value is 5 minutes), the device configuration will return to the state before the last **commit** command execution. You can roll back configuration changes before the timer expires. To do that, use the **restore** command.

9.3 Creating Configuration Backup

Configuration backups allow the access node operation to be quickly restored after abnormal situations or replacement. Manual or triggered (on events) creation of backups is recommended at a regular basis.

Access node configuration is uploaded to a TFTP server available in management network. The **copy** command is used to upload the data. Pass the uploaded device configuration **fs://backup** and destination URI as parameters.

```
ma4000# copy fs://backup tftp://192.168.22.1/config
```

To create backups automatically, you have to configure special events (triggers).

Step 1. If necessary, define the configuration backup upload on each change (on **commit** command execution) with the **backup onchange** command.

```
ma4000(config)# backup onchange
```

Step 2. If necessary, define the configuration backup upload on timer with the **backup ontimer** command. Set the configuration backup upload timer with the **backup ontimer-period** command. Pass the timer value in seconds as a parameter.

```
ma4000(config)# backup ontimer
ma4000(config)# backup ontimer-period 3600
```

Step 3. Specify the URI for configuration upload.

```
ma4000(config)# backup path tftp://192.168.22.1/config
```

Step 4. Apply and confirm changes.

```
ma4000(config)# do commit
ma4000(config)# do confirm
```

9.4 Configuration Restore

Access node configuration is restored from a TFTP server available in management network. Use **copy** command to restore the data.

Step 1. Load configuration using the **copy** command. Pass the restored configuration source URI and **fs://backup** as parameters.

```
ma4000# copy tftp:// 192.168.22.1/config fs://backup
```

Step 2. Apply and confirm changes.

```
ma4000# commit
ma4000# confirm
```

9.5 Configuration Reset

To reset the access node configuration to factory settings, use the **default** command.

```
ma4000# default
Entire candidate configuration will be reset to default, all settings will be
lost upon commit. Additional firmware will be deleted.
Do you really want to continue ? y/n y
```

10 NETWORK SETTINGS

10.1 Introduction

This chapter describes adjustment of network settings for an access node. Adjusting network settings enables remote control and integration with OSS/BSS systems.

10.2 Adjustment of Network Settings

Adjustments of network settings are recommended to be done via COM port connection, described under [7.2 Connecting to CLI via COM Port](#). This will prevent issues with connection loss before the access node being adjusted. Be very careful when using remote adjustment.

Step 1. Use the **show management** command to view the current network settings.

```
ma4000#show management
Network parameters :
    ip             192.168.0.1
    mask           255.255.255.0
    gateway        192.168.0.254
    vlan           1
```

Step 2. . Switch to the **configure view** and set the access node name by using the **hostname** command.

```
ma4000# configure terminal
ma4000(config)# hostname ma4000
```

Step 3. Set the access node IP address by using the **management ip** command. Pass the IP address and the subnet mask as parameters.

```
ma4000(config)# management ip 192.168.22.22 255.0.0.0
```

Step 4. Set the default gateway by using the **management gateway** command.

```
ma4000(config)# management gateway 192.168.22.254
```

Step 5. Adjust the VLAN management of the access node by using the **management vlan** command, if necessary.

```
ma4000(config)# management vlan 9
```

Proper operation of the inband management function requires VLAN adjustment in the switch view as described in [13 VLAN Configuration](#), page 56.

Step 6. Set the lifetime of MAC addresses by using the **mac address-table aging-time** command. Pass time in seconds as a parameter.

```
ma4000(config)# mac address-table aging-time 600
```

Step 7. The network settings change as soon as the configuration is applied. No terminal reboot is needed.

```
ma4000(config)# do commit
ma4000(config)# do confirm
```

11 USER MANAGEMENT

11.1 Introduction

This Chapter is devoted to management of the access node users.



The factory settings provide only for one user, i.e. the device administrator.

login: *admin*

password: *password*

When you start to configure the access node, we recommend you to change the password of the "admin" user.

For security reasons, access node users should be delegated with a strict rule set. For these purposes, each user gets his own access level. Level 0 corresponds to a minimum rule set, Level 15—to a maximum rule set. Commands available to the user will correspond to his/her privilege level. Privilege list and description:

- view-switch: allows to view PP4X switch and slot configuration.
- view-alarm: allows to view active alarms, their configuration and event log.
- view-system: allows to view system settings: logging, user configuration, Tacacs;
- view-general: allows to view basic settings: management, firmware information, status of boards and log message reading;
- view-gpon: allows to view configuration and status of OLT chips, GPON ports, and OLT;
- view-ont: allows to view MAC tables and ONT counters;
- view-ont-profile: allows to view ONT profile configuration;
- view-switch-interfaces: enables Ethernet interface operation monitoring: counters; Ethernet port status, utilization and configuration; MAC table configuration;
- config-switch : enables switch configuration: LACP, QoS, STP;
- config-alarm: enables alarm configuration;
- config-system: enables configuration of system parameters: logging, user configuration, Tacacs;
- config-general: enables configuration of management parameters and operations with software;
- config-gpon: enables configuration of OLT profiles and configuration of OLT chip basic operation parameters;
- config-ont: enables ONT configuration: adding, removing, service activation;
- ont-operation: allows to execute specific ONT management commands: reboot, reconfiguration, firmware update;
- config-ont-profile: enables configuration of ONT profiles ;
- config-switch-interfaces: enables Ethernet interface configuration: aggregation, enabling/disabling, VLAN operations.

11.2 User List Preview

In order to view the user list, use the **show users config** command:

```
ma4000# show users config
```

```

    System users
    ~~~~~
User name          User privilege level
-----
root               15
admin              15
remote             15
linux              0
4 system users.
```

The "admin", "root" and "linux" users always exist and cannot be deleted or duplicated. The access node supports up to 16 users.

11.3 Adding a New User

In order to operate effectively and safely, the access node, as a rule, requires one or several additional users. For adding new users, use the **user** command in the **configure view**:

```
ma4000(config)# user operator
ma4000(config)# do commit
ma4000(config)# do show users
```

```

    System users
    ~~~~~
User name          User privilege level
-----
root               15
admin              15
remote             15
linux              0
operator           0
5 system users.
```

Pass the name of the new user to the **user** command as a parameter. The name should not be longer than 32 characters. The name should not contain special characters.

11.4 Changing User Password

For changing user's password, use the **user** command. Pass a user name and new password as a parameters.

```
ma4000(config)# user operator password newpassword
```

The password should not be longer than 31 characters. If the password contains a space, quotations should be used for the password.

11.5 Viewing and Changing User Access Rights

To manage user access rights, user priority system is implemented.

When a user is created, minimal rights are delegated to him:

```
ma4000(config)# user operator
ma4000(config)# do show users
```

```
System users
~~~~~
User name          User privilege level
-----
root               15
admin              15
remote             15
linux              0
operator           0
5 system users.
```

To change user password, use the **user** command. Pass the user name and the new password as parameters.

```
ma4000(config)# user operator privilege 15
ma4000(config)# do show users
```

```
System users
~~~~~
User name          User privilege level
-----
root               15
admin              15
remote             15
linux              0
operator           15
5 system users.
```

11.6 Deleting a User

For deleting a user, use the **no user** command in the **configure view**. The command takes the user's name as a parameter:

```
ma4000# configure terminal
ma4000(config)# no user operator
ma4000(config)# do commit
```

11.7 User Session Configuration

Timeouts are used to limit the duration of CLI sessions. If no commands are executed before the timeout, the session will be closed automatically. Use the **cli session-timeout** from the **configure view** command. Pass the time period in minutes as a parameter.

```
ma4000(config)# cli session-timeout 300
```

11.8 User Authentication Configuration

There are several methods of user authentication in the system:

- do not use the authentication;
- local — use local user database for authentication;
- tacacs+ — use TACACS+ server for authentication;
- radius — use RADIUS server for authentication;

Step 1. Define the default authentication procedure using the **aaa authentication login** command.

```
ma4000(config)# aaa authentication login default tacacs+ local
```

In this example, the system will attempt to perform authentication using the Tacacs+ server in the first place (see Section [12.5 Tacacs/Tacacs+ Configuration](#)). If the server is unavailable, the authentication will be performed using the local user database.

Step 2. Switch to configuration of the connection method, e.g. the console.

```
ma4000(config)# line console
```

Step 3. Define the authentication procedure for the selected method. You can use the default authentication procedure or a custom procedure, created by analogy to the Step 1.

```
ma4000(config)# line console  
ma4000(config-line-console)# login authentication default
```

Step 4. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

12 SERVICE CONFIGURATION

12.1 SNMP Configuration

Step 1. Enable SNMP agent using the **ip snmp agent enable** command:

```
ma4000(config)# ip snmp agent enable
```

Step 2. Define the SNMP device name using the **ip snmp agent system name** command:

```
ma4000(config)# ip snmp agent system name ma4000
```

Step 3. Define SNMPv3 EngineID:

```
ma4000(config)# ip snmp agent engine id test
```

Step 4. Define the SNMP trap destination server. Pass SNMP Trap version and destination IP address as parameters.

```
ma4000(config)# ip snmp agent traps informs 192.168.1.100
```

Step 5. Define SNMPv2 community, if necessary.

```
ma4000(config)# ip snmp agent community readonly public
```

Step 6. Add SNMPv3 users using the **ip snmp agent user add** command. Pass username, password (8-31 symbols) and access mode as parameters.

```
ma4000(config)# ip snmp agent user add test test ro
```

Step 7. Apply the configuration using the **commit** command:

```
ma4000(config)# do commit
```

12.2 System Log Configuration

Step 1. Define the level of messages, that will be sent to the console and the remote CLI sessions (SSH and Telnet).

```
ma4000(config)# logging console debug
ma4000(config)# logging monitor debug
```

Step 2. Define the maximum system log file size. When the file size is exceeded, the system will perform the rotation.

```
ma4000(config)# logging file-size 1000
```

Step 3. Define the quantity of system log files of the same type.

```
ma4000(config)# logging max-files 5
```

Step 4. If necessary, perform the message level configuration for the files listed in the Table 25.

```
ma4000(config)# logging file pp debug
```

Step 5. If necessary, perform the message filter configuration for the files listed in the Table 25 using the **match** command. Use **destination** command to define the destination for messages.

```
ma4000(config)# logging builtin-filter pp
ma4000(config-log-filter-pp)# match pp
ma4000(config-log-filter-pp)# destination file pp
ma4000(config-log-filter-pp)# destination host 192.168.1.100 port 55 transport
udp
```

Step 6. If necessary, enable system log message forwarding to the remote SYSLOG server.

```
ma4000(config-log-filter-pp)# exit
ma4000(config)# logging host 192.168.1.120 port 55 transport udp debug
```

Step 7. If necessary, enable the system log file storage to the non-volatile memory.

```
ma4000(config)# logging storage persistent
```

Step 8. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

12.3 SSH Configuration

Step 1. Enable SSH server using the **ip ssh server** command.

```
ma4000(config)# ip ssh server
```

Step 2. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

12.4 Telnet Configuration

Step 1. Enable Telnet server using the **ip telnet server** command.

```
ma4000(config)# ip telnet server
```

Step 2. Specify the connection port using the **ip telnet port** command.

```
ma4000(config)# ip telnet port 9000
```

Step 3. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

12.5 Tacacs/Tacacs+ Configuration

Step 1. Define the Tacacs server connection settings.

```
ma4000(config)# tacacs-server timeout 10
ma4000(config)# tacacs-server key 12345
ma4000(config)# tacacs-server encrypted key 98C7D37909
```

Step 2. Add Tacacs server into the list of utilized servers using the **tacacs-server host** command. Define the connection settings for this server.

```
ma4000(config)# tacacs-server host 192.168.1.200
ma4000(config-tacacs)# key 123
ma4000(config-tacacs)# timeout 12
ma4000(config-tacacs)# priority 0
ma4000(config-tacacs)# port-number 3000
```

Step 3. If necessary, enable accounting for commands entered by the user.

```
ma4000(config)# aaa accounting commands tacacs+
```

Step 4. If necessary, enable accounting for user logins/logouts.

```
ma4000(config)# aaa accounting start-stop tacacs+
```

Step 5. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

12.6 Radius configuration

Step 1. Define common parameters of connection to Radius servers.

```
ma4000(config)# radius-server timeout 10
ma4000(config)# radius-server key 12345
ma4000(config)# radius-server encrypted key 98C7D37909
```

Step 2. Add Radius server to the used servers list by **radius-server host** command. Define parameters of connection to the server.

```
ma4000(config)# radius-server host 192.168.1.200
ma4000(config-radius)# key 123
ma4000(config-radius)# timeout 12
ma4000(config-radius)# priority 0
ma4000(config-radius)# port-number 3000
```

Step 3. Apply the configuration by commit command.

```
ma4000(config)# do commit
```

12.7 SNTP Configuration

Step 1. Enable time synchronization using the **ip sntp client** command.

```
ma4000(config)# ip sntp client
```

Step 2. Define the time synchronization server IP address using the **ip sntp server** command:

```
ma4000(config)# ip sntp server 192.168.1.254
```

Step 3. Specify the synchronization interval in minutes:

```
ma4000(config)# ip sntp poll-period 60
```

Step 4. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

13 VLAN CONFIGURATION

13.1 Introduction

This Chapter describes VLAN configuration in the access node.

VLAN (Virtual Local Area Network) is a group of devices which communicate on channel level and are combined into a virtual network that is connected to one or more network devices (GPON terminals or switches). VLAN is a very important tool for creating a flexible and configurable logical network topology over the physical topology of a GPON network.

VLAN has two or more switch interfaces. A VLAN interface may be either tagged or untagged. An outgoing packet of a tagged interface has a VLAN tag. An outgoing packet of an untagged interface has no VLAN tags. For more details on interfaces configuration and rules refer to [15 Interfaces Configuration](#).

13.2 Adding a VLAN

Step 1. Switch to the access node **configure view**.

```
ma4000# configure terminal
```

Step 2. Add a VLAN by using the **vlan** command. Pass VID as a parameter.

```
ma4000(config)# vlan 100
```



CLI automatically switches view to work with the VLAN. The same command is used to configure existing VLANs.

13.3 VLAN Configuration

Step 1. Add tagged interfaces with the help of the "tagged" command. Pass interface type and number (or a range) as parameters. The interface types and numbers are given in Table 14.

```
ma4000(vlan-100)# tagged front-port 1/0
```

Step 2. Add untagged interfaces by using the **untagged** command if needed. Pass interface type and number (or a range) as parameters.

```
ma4000(vlan-100)# untagged front-port 1/1
```

Step 3. Delete all unnecessary interfaces from VLAN with the help of the **forbidden** command. Pass interface type and number (or a range) as parameters.

```
ma4000(vlan-100)# forbidden front-port 1/2-3
```


Step 4. Enable IGMP snooping by using the **ip igmp snooping slot <slot> enable** command if necessary.

```
ma4000(vlan-100)# ip igmp snooping slot 0-15 enable
ma4000(vlan-100)# ip igmp snooping pp4x enable
```

Step 5. Enable IGMP querier by using the **ip igmp snooping querier enable** command if necessary.

```
ma4000(vlan-100)# ip igmp snooping querier enable
```

Step 6. For further convenience, specify VLAN name by using the **name** command. To clear the name, use the **no name** command. The default name is VID.

```
ma4000(vlan-100)# name iptv
```

Step 7. Apply the configuration by using the **commit** command.

```
ma4000(vlan-100)# do commit
```

13.4 Deleting a VLAN

Step 1. Delete a VLAN by using the **no vlan** command. Pass VID (or its range) as a parameter.

```
ma4000(config)# no vlan 100
```

Step 2. Apply the configuration by using the **commit** command.

```
ma4000(config)# do commit
```

14 PP4X STACKING CONFIGURATION

If two PP4X modules are used , their configuration files will be synchronized. If PP4X master fails, PP4X slave will keep the running configuration.

The **no stack sync-allow** command allows to disable the configuration file synchronization for the stack.

If the configuration file synchronization is disabled, PP4X slave will be able to get and apply the configuration from the master device, but will not be able to save it to its own file system for the future use.

Enable the synchronization of configuration files using the **stack sync-allow** command:

```
ma4000# stack sync-allow
Command accepted. Automatic synchronization (if needed) will be performed in the
background shortly.
```

15 INTERFACES CONFIGURATION

15.1 Introduction

This Chapter describes the configuration of the access node interfaces.

Access node interfaces can be divided into two groups: Ethernet interfaces and GPON interfaces. Ethernet interfaces are used for access node connection to operator's network core. GPON interfaces are used for ONT connections.

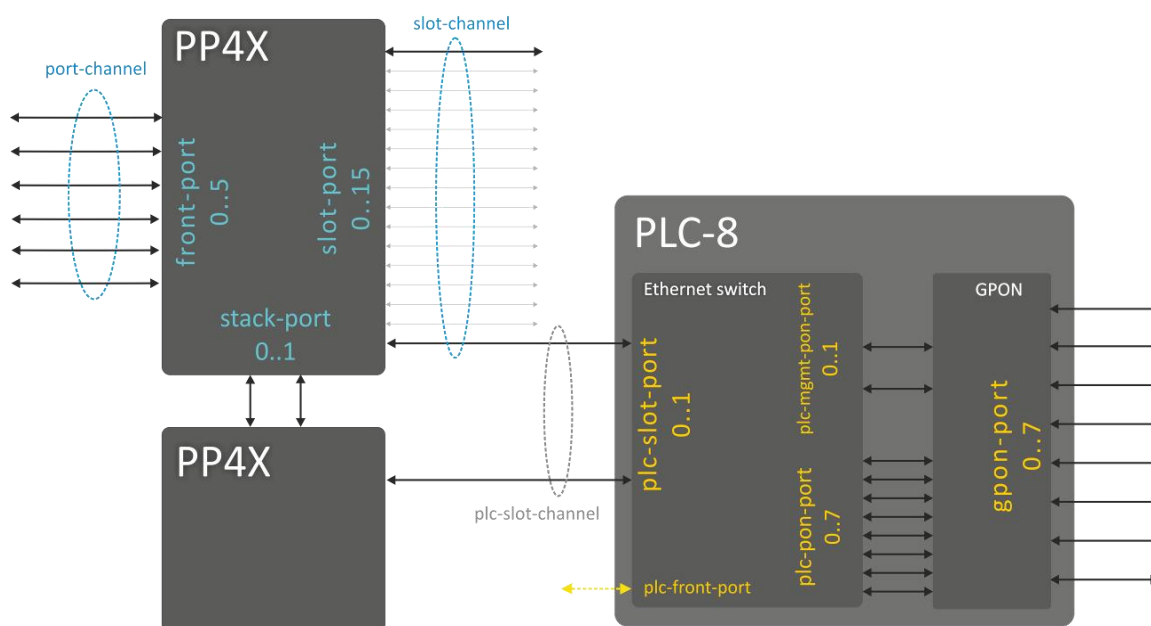


Fig. 23—Access node interface name system

For accepted access node interface name system, see Table 14.

Table 14—Access node interface name system and numbering

Interface name	Description	Range
front-port	PP4X module external uplink interfaces	Specified as: U/P U—PP4X module number [1 .. 2] P—PP4X uplink interface number [0..5]
port-channel	LAG of PP4X module uplink interfaces	[1..8]—aggregation group number
slot-port	PP4X module interface for PLC8 GPON module connection.	Specified as: U/P U—PP4X module number [1 .. 2] P—interface number for PLC8 module [0..15]
slot-channel	LAG of PP4X module interfaces for PLC8 modules	[0..15]—PLC8 module number
stack-port	PP4X module internal stacking interfaces	Specified as: U/P U—PP4X module number [1 .. 2] P—interface number for PP4X module [0..1]
plc-slot-port	PLC8 module interfaces for connection to central switches—PP4X modules	Specified as: S/P S—PLC8 module version [0 .. 15] P—interface number for PP4X module [0..1]

plc-slot-channel	PLC8 module interface LAG for connection to central switches—PP4X modules	Specified as: S/P S—PLC8 module number [0..15] P—channel number for module [0]
plc-front-port	PLC8 module external management interface (mgmt)	Specified as: S/P S—PLC8 module number [0..15] P—channel number for module [0]
plc-pon-port	PLC8 switch falling interface, connected to OLT GPON	Specified as: S P S—PLC8 module version [0 .. 15] P—port number [0..7]
plc-mgmt-pon-port	PLC8 switch falling interface, connected to OLT GPON, and designed for management purposes	Specified as: S P S—PLC8 module version [0 .. 15] P—port number [0..1]
gpon-port	PLC8 module external GPON interfaces	Specified as: S P S—PLC8 module version [0 .. 15] P—port number [0..7]
ont	Interfaces for the subscriber-side ONT terminals	Specified as: S/P/I S—PLC8 module number [0..15] P—PLC8 module port number [0..7] I—ONT interface number [0..63]

15.2 Ethernet Interfaces Configuration

Step 1. Switch to the view of the interface (of interface group) which settings should be changed.

```
ma4000(config)# interface front-port 1/0
```

Step 2. Enable the interface by using the **no shutdown** command. The **shutdown** command disables the interface.

```
ma4000(front-port-1/0)# no shutdown
```

Step 3. Enable or disable flow control (IEEE 802.3x PAUSE) by using the **flow-control** command.

```
ma4000(front-port-1/0)# flow-control on
```

Step 4. Enable or disable ingress filtering by using the **ingress-filtering** command. Only the packets of the VLANs having this interface will pass the enabled filter. Other packets will be filtered out. If the filtering is disabled, a packet will be processed regardless of its VID field.

```
ma4000(front-port-1/0)# ingress-filtering
```

Step 5. Specify a rule for VLAN tags processing for incoming packets by using the **frame-types** command. As a parameter, specify the packets to be allowed: either **tagged** (tagged only) or **all** (both tagged and untagged).

```
ma4000(front-port-1/0)# frame-types tagged
```

Step 6. Specify port **pvid**, i. e. the VLAN which will accommodate untagged packets.

```
ma4000(front-port-1/0)# pvid 100
```

Step 7. If necessary, enable or disable the capability to send packets from this interface to another one (or a range of interfaces) by using the **bridging to** command. Pass interface type and number (or a range) as parameters. The interface types and numbers are given in [Table 14](#).

```
ma4000(front-port-1/0)# bridging to front-port 1/1
```

Step 8. Set automatic determination of speed and duplex of the interface either by using the **speed auto** command or manually.

```
ma4000(front-port-1/0)# speed auto
```

Step 9. Apply the configuration using the **commit** command.

```
ma4000(front-port-1/0)# do commit
```

15.3 GPON Interfaces Configuration

Step 1. Switch to the **configure view**.

```
ma4000# configure terminal
```

Step 2. Activate traffic encryption with the **gpon olt encryption** command, if necessary. Specify encryption key renewal period with the **gpon olt encryption key-update** command. Pass the time period in seconds as a parameter.

```
ma4000(config)# gpon olt encryption
ma4000(config)# gpon olt encryption key-update 60
```

Step 3. Specify ONT authentication method with the **gpon olt authentication** command.

```
ma4000(config)# gpon olt authentication both
```

Step 4. Switch to GPON interface configuration.

```
ma4000(config)# interface gpon-port 0-7
```

Step 5. Enable or disable interfaces with the **no shutdown** or **shutdown** command respectively, if necessary.

```
ma4000(config)(if-gpon-0-7)# no shutdown
```

Step 6. Activate FEC for the interface with the **fec** command, if necessary.

```
ma4000(config)(if-gpon-0-7)# fec
```

Step 7. Adjust time settings of optical transceiver if needed.

```
ma4000(config)(if-gpon-0-7)# optics use-custom
ma4000(config)(if-gpon-0-7)# optics ...
```



Optical transceiver should be adjusted only by agreement with Eltex Service Center.

Step 8. Apply the configuration by using the **commit** command.

```
ma4000(config)(if-gpon-0-7)# do commit
```

16 ISOLATION GROUP CONFIGURATION

16.1 Introduction

Isolation group is the mechanism, that allows to restrict the traffic flow inside the VLAN. Isolation groups allow to configure one-way data transmission or divide interfaces located inside the VLAN into 2 logical groups. Operating principle is shown in Fig. 24.

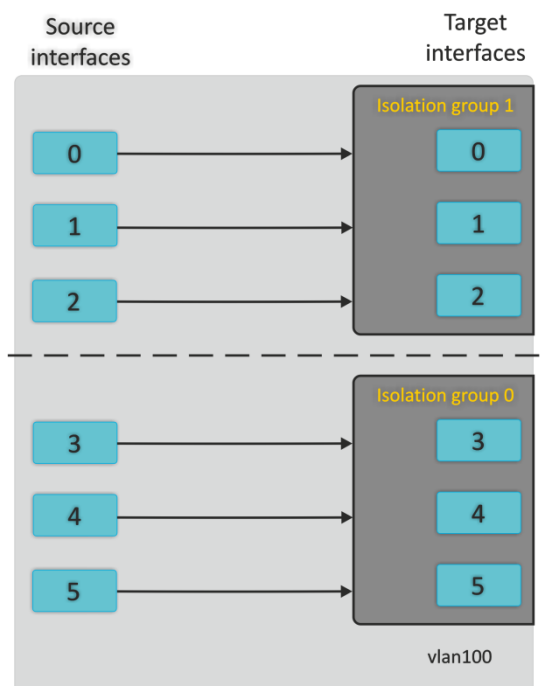


Fig. 24—Isolation group operating principle

16.2 Isolation Group Configuration

Step 1. Specify the interface isolation group using the **isolation group** command. Pass the isolation group number as a parameter:

```
ma4000(config)# isolation group 0
```

Step 2. Add the required number of destination interfaces into the group using the **allow** command:

```
ma4000(pp4x-config-isolation-0)# allow front-port 1/0-2
```

Step 3. Repeat Steps 1 and 2 for another group:

```
ma4000(pp4x-config-isolation-0)# exit
ma4000(config)# isolation group 1
ma4000(pp4x-config-isolation-1)# allow front-port 1/3-5
```

Step 4. Go to the configuration mode for the required VLAN:

```
ma4000(pp4x-config-isolation-1)# exit  
ma4000(config)# vlan 100
```

Step 5. Enable isolation with the **isolation enable** command:

```
ma4000(vlan-100)# isolation enable
```

Step 6. Enable the data transmission from the specific interface to the isolation group (destination interfaces) using the **isolation assign** command. Pass the source interface name and the isolation group number as parameters:

```
ma4000(vlan-100)# isolation assign front-port 1/0-2 group 0  
ma4000(vlan-100)# isolation assign front-port 1/3-5 group 1
```

Step 7. Apply the configuration using the **commit** command:

```
ma4000(vlan-100)# do commit
```

17 SELECTIVE Q-IN-Q CONFIGURATION

17.1 Introduction

SELECTIVE Q-IN-Q function allows to assign external SPVLAN (Service Provider's VLAN), substitute Customer VLAN, and block the transmission of traffic based on configured filtering rules by internal VLAN numbers (Customer VLAN).

17.2 Selective Q-in-Q Configuration

Step 1. Switch to the selective Q-in-Q configuration mode.

```
ma4000# configure terminal
ma4000(config)# selective-qinq common
ma4000(config-selective-qinq)#
```



You can create only 1024 rules Selective Q-in-Q for PP4X board. To cover larger numbers of CVLANs, use 'ignore' function.

Step 2. Add external tag adding rules with the **add-tag** command. Pass the external tag VID and internal tag VID or range as parameters.

```
ma4000(config-selective-qinq)# add-tag svlan 20 cvlan 100-200
ma4000(config-selective-qinq)# add-tag svlan 30 cvlan ignore
```

Such configuration implies, that packets coming to an interface with CVLAN 100-200 tag will have the external tag 20 added to them, and all other packets falling outside the scope of this rule will have the external tag 30 added. Rules with 'ignore' option have a lower priority compared to rules with explicitly assigned CVLAN.

Step 3. And/or add VLAN translation rules.

```
ma4000(config-selective-qinq)# overwrite-tag new-vlan 1000 old-vlan 2000 ingress
ma4000(config-selective-qinq)# overwrite-tag new-vlan 2000 old-vlan 1000 egress
```

Step 4. Switch to the configuration of interfaces, that should use the selective Q-in-Q. Enable the function using the **selective-qinq enable** command.

```
ma4000(config-selective-qinq)# exit
ma4000(config)# interface front-port 1/3-5
ma4000(front-port-1/3-5)# selective-qinq enable
```

Step 5. Apply the configuration using the **commit** command.

```
ma4000(front-port-1/3-5)# do commit
```



If the global Q-in-Q rule table is not sufficient for the purpose, and different interfaces require different settings, you should use Q-in-Q rule lists. You can configure these lists in the separate selective-qinq list <name> by analogy to the sequence shown. To assign the list for the interfaces, use the 'selective-qinq list <name>' command.

18 QOS CONFIGURATION

The traffic prioritization method will be chosen depending on the configured system rules (IEEE 802.1p/DSCP).

Table 15—Traffic prioritization methods

Priority	Description
0	All priorities are equal
1	Packet selection is based on IEEE 802.1p standard
2	Packet selection is based on IP ToS (type of service) at the level 3 only—Differentiated Services Codepoint (DSCP) support
3	Interactions based on 802.1p or DSCP/TOS

Step 1. Define the queue, that will be used for packets without any preconfigured rules. Queue 0 has the lowest priority.

```
ma4000(config)# qos default 0 slot 0
```

Step 2. Specify the traffic prioritization method using the **qos type** command. Pass the prioritization type as a parameter (see Table 15):

```
ma4000(config)# qos type 1 slot 0
```

Step 3. Use the **qos map** command to specify rules of 802.1p and DSCP/TOS translation into the queue number. Pass the field type and priority list as parameters:

```
ma4000(config)# qos map 1 0-4,15,63 to 6
ma4000(config)# do show qos
Priority assignment by NONE packet field, all priorities are equal
Default priority queue is 0
DSCP/TOS queues:
0:
1:
2:
3:
4:
5:
6: 0-4,15,63
802.1p queues:
0:
1:
2:
3:
4:
5:
6:
```

Step 4. Apply the configuration using the **commit** command:

```
ma4000(config)# do commit
```

19 LAG CONFIGURATION

19.1 Introduction

This Chapter describes configuration of uplink interfaces aggregation.

Link aggregation (IEEE 802.3ad) is a technology that allows multiple physical links to be combined into one logical link (aggregation group). Aggregation group has high throughput and is very reliable.

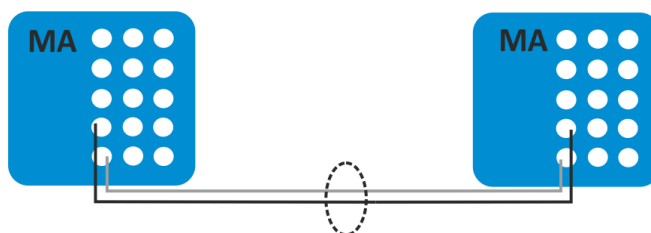


Fig. 25—Multiple Physical Links Combined to an Aggregation Group

The access node supports two interface aggregation modes: static and dynamic. Static aggregation implies that all communication links of a group are always active. As for dynamic aggregation, link activity is dynamically determined during operation via LACP protocol.

Table 16—Operation Modes of Aggregation Groups

Mode	Description
static	Link aggregation protocol is not used
lacp	LACP is used

The access node has several algorithms to balance load within aggregation groups.

Table 17—Load Balance Modes

Mode	Description
ip	Based on IP address of sender and receiver
ip-l4	Based on IP address of sender and receiver, and L4
mac	Based on MAC address of sender and receiver
mac-ip	Based on MAC and IP addresses of sender and receiver
mac-ip-l4	Based on MAC address, IP address and L4 of sender and receiver

The access node supports two LACP modes. Passive mode—the access node does not initiate creation of a logical link, but processes incoming LACP packets. Active mode—the access node creates an aggregated communication link and initiates parameters conformance. The parameters are coordinated in case equipment operates in active or passive LACP modes.

19.2 LAG Configuration

LAG configuration represents static aggregation configuration or LACP configuration. To configure LAG, perform the steps marked blue in figure 26. LACP configuration requires all steps to be performed.

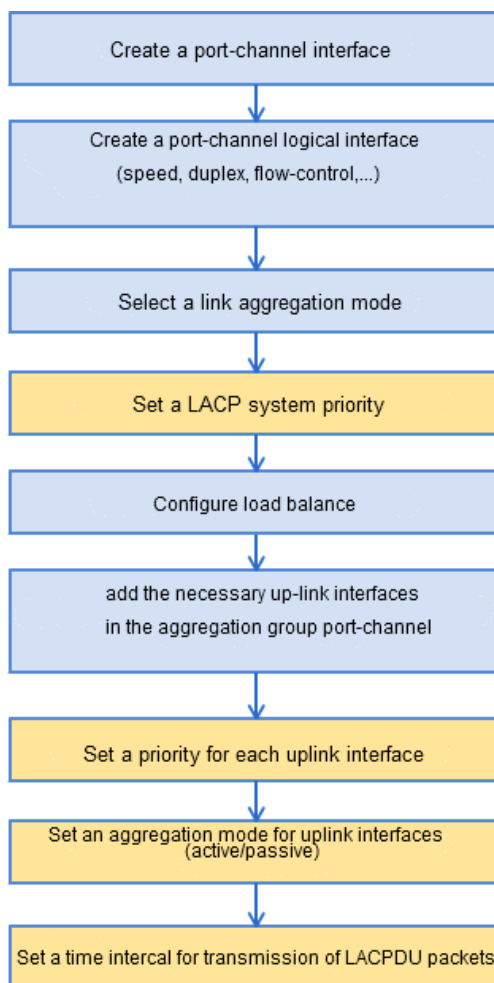


Fig. 26—LAG and LACP Configuration Procedure

Step 1. Create a **port-channel** logical interface by using the **interface port-channel** command.

As a parameter, pass the number of the interface being created. You can create up to eight logical interfaces.

```
ma4000(config)# interface port-channel 1
ma4000(express-config-port-channel-1) #
```

Step 2. Set general interface parameters: speed, duplex, flow-control, etc. Interfaces configuration is described in details in [15 Interfaces Configuration](#).

Step 3. Set an aggregation mode by using the **mode** command. Pass the operation mode as a parameter. Operation modes are specified in [Table 16](#).

```
ma4000(express-config-port-channel-1) # mode lacp
```

Step 4. This step should only be performed for LACP configuration. Set a LACP system priority by using the **lacp system-priority** command. The **no lacp system-priority** command returns 32768 by default.

```
ma4000(express-config-port-channel-1)#exit
ma4000(config)# lacp system-priority 32768
```

Step 5. Specify load balance rules with the help of the "port-channel load-balance" command if needed. Pass the balance mode as a parameter. Balance modes are specified in [Table 17](#).

```
ma4000(config)# port-channel load-balance ip
```

Step 6. Add physical interfaces into the logical one by using the **channel-group** command. As a parameter, pass the number of the logical interface.

```
ma4000(config)# interface front-port 1/3-5
ma4000(front-port-1/3-5)# channel-group 1 normal
```

Step 7. This step should only be performed for LACP configuration. Set a priority for the physical interface with the help of the **lacp port-priority** command if necessary. The **no lacp port-priority** command resets port priority to the default value of 32768; 1 is the highest priority.

```
ma4000(front-port-1/3-5)# no lacp port-priority
ma4000(front-port-1/3-5)# exit
ma4000(config)# interface front-port 1/3
ma4000(front-port-1/3)# lacp port-priority 256
```

Step 8. This step should only be performed for LACP configuration. Use the **lacp mode** command to set an active or passive LACP mode.

```
ma4000(front-port-1/3)# exit
ma4000(config)# interface front-port 1/3-5
ma4000(front-port-1/3-5)# lacp mode active
```

Step 9. This step should only be performed for LACP configuration. In case of the active LACP mode, set an interval for transmission of LACP control packets with the help of the **lacp rate** command. Pass slow (30 seconds) or fast (1 second) as a parameter.

```
ma4000(front-port-1/3-5)# lacp rate slow
```

Step 10. Apply the configuration by using the **commit** command.

```
ma4000(front-port-1/3-5)# do commit
```

20 SPANNING TREE CONFIGURATION

20.1 Introduction

Spanning Tree Protocol (STP) is a network protocol. The main task of STP is to eliminate loops in the arbitrary Ethernet network topology with one or multiple network bridges connected with redundant links. STP solves this task by automatically blocking connections that are redundant for the full switch interconnection at the given moment of time.

Spanning Tree configuration may be applied globally, or for selected front interfaces of LAGs only.

20.2 Spanning Tree Configuration

Step 1. Enable STP with the **spanning-tree enable** command:

```
ma4000(config)# spanning-tree enable
```

Step 2. Define the spanning tree protocol type: STP or RSTP:

```
ma4000(config)# spanning-tree mode rstp
```

Step 3. Define the command forwarding delay using the **spanning-tree fdelay** command. Forwarding delay is the time, during which the port remains in Listening and Learning states prior to going into Forwarding state:

```
ma4000(config)# spanning-tree fdelay 10
```

Step 4. Specify the sending time for hello packets using the **spanning-tree hello** command:

```
ma4000(config)# spanning-tree hello 21
```

Step 5. Define the STP bridge priority using the **spanning-tree priority** command.

```
ma4000(config)# spanning-tree priority 4096
```

Step 6. Specify the route value for various interfaces:

```
ma4000(config)# interface front-port 1/3
ma4000(front-port-1/3)# spanning-tree pathcost 1
ma4000(front-port-1/3)# exit
ma4000(config)# interface front-port 1/4
ma4000(front-port-1/4)# spanning-tree pathcost 2
ma4000(front-port-1/4)# exit
```

Step 7. Define BPDU packet processing mode by the interface with disabled STP protocol.

Pass the operation mode as a parameter.

¹ Not supported in the current firmware version. The default value is 2

- filtering—packets are filtered for the interface with STP BPDU protocol disabled
- flooding—untagged BPDU packets are transmitted for the interface with STP protocol disabled, tagged packets are filtered

```
ma4000(config)# spanning-tree bpdu flooding
```

Step 8. Define the maximum quantity of BPDU packets, that could be received by the device in a second of time, using the **spanning-tree holdcount** command:

```
ma4000(config)# spanning-tree holdcount 5
```

Step 9. If necessary, specify the BPDU packet timeout using the **spanning-tree maxage** command:

```
ma4000(config)# spanning-tree maxage 15
```

Step 10. If necessary, define the connection type as the edge link to the host (on configurable port/ports). In this case, data transmission is enabled automatically for the port, when the link is established.

```
ma4000(front-port 1/1)# spanning-tree admin-edge
```

Step 11. If necessary, define the automatic bridge identification for configured port(s).

```
ma4000(front-port 1/1)# spanning-tree auto-edge
```

Step 12. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

21 DUAL HOMING CONFIGURATION

21.1 Introduction

The operating principle of *Dual Homing* technology is similar to the Spanning Tree technology. However, the Spanning Tree technology has a major disadvantage. If there are more than 7 computers in a network, fault identification and performance restoration can take up to several minutes. During this time, the network will not be available. While it may not be significant for office networks, loss of control for several minutes at production and transportation facilities, and financial institutions may lead to catastrophe.

In case of Dual Homing technology, these operations will take up just 3 seconds.

21.2 Dual Homing Configuration

Step 1. Switch to the selected interface or interface group configuration:

```
ma4000(config)# interface front-port 1/3
```

Step 2. Specify the reserved interface, that will be used for communication fallback, when the main connection is lost.



You can enable reservation only for those interfaces, where SPANNING TREE protocol is disabled and VLAN Ingress Filtering is enabled. If the reserve is specified globally for the interface, it will be used for all VLANs. If another reserve is specified for some VLANs, this setting will take priority over the global setting.

```
ma4000(front-port-1/3)# backup interface front-port-1/4 vlan 10
```

Step 3. Specify the packet quantity per second, that will be sent into the active interface during the fallback:

```
ma4000(front-port-1/3)# exit
ma4000(config)# backup-interface mac-per-second 200
```

Step 4. Specify the quantity of packet copies per second, that will be sent into the active interface during the fallback:

```
ma4000(config)# backup-interface mac-duplicate 4
```

Step 5. If necessary, configure the switching to the main interface, when the communication is restored.

```
ma4000(config)# backup-interface preemption
```

Step 6. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

22 LLDP CONFIGURATION

22.1 Introduction

Link Layer Discovery Protocol (LLDP) is a data-link level protocol, that allows network devices to announce the information on their essence and capabilities into the network and gather such information from the neighbouring devices.

22.2 LLDP Configuration

Step 1. Enable LLDP for operation using **lldp enable** command:

```
ma4000(config)# lldp enable
```

Step 2. Define the amount of time for the receiving device to keep LLDP packets before dropping them.

```
ma4000(config)# lldp hold-multiplier 5
```



This value will be transmitted to the receiving side in LLDP update packets; is a divisibility for LLDP timer. Thus, LLDP packet lifetime is calculated by the equation: $TTL = \min(65535, LLDP-Timer * LLDP-HoldMultiplier)$.

Step 3. Define the LLDP reinitialization time:

```
ma4000(config)# lldp reinit 3
```

Step 4. Define the frequency of LLDP information updates sent by the device:

```
ma4000(config)# lldp timer 60
```

Step 5. Define the delay between the subsequent LLDP packet transmissions, initiated by changes of values or status in local LLDP MIB database.

```
ma4000(config)# lldp tx-delay 3
```



It is recommended to set this delay less than $0.25 * LLDP-Timer$.

Step 6. Define the LLDP packet processing mode:



LLDP packet processing mode:

- **filtering**—LLDP packets are filtered, if LLDP is disabled on the switch
- **flooding**—LLDP packets are transmitted, if LLDP is disabled on the switch

```
ma4000(config)# lldp lldpdu flooding
```

Step 7. Apply the configuration using the **commit** command:

```
ma4000(config)# do commit
```


23 MULTICAST CONFIGURATION

23.1 Introduction

The Chapter describes peculiarities of IPTV service configuration.

Internet Group Management Protocol (IGMP) and *MLD (Multicast Listener Discovery)* are used in hosts and routers for multicasting support. It provides all systems of a physical network with relevant information: which hosts are included in groups and which group corresponds to a host.

IGMP snooping is a technique that allows network devices of the channel level (switches) to snoop IGMP requests from hosts to a group router in order to decide whether group traffic transmission to the corresponding interfaces should be started or stopped. When a switch snoops a host's IGMP request for connection to a multicast group, it adds the port the host is connected to into the group (for group traffic retranslation). And vice versa, having snooped a "leave_group" request, the switch removes the corresponding port from the group.

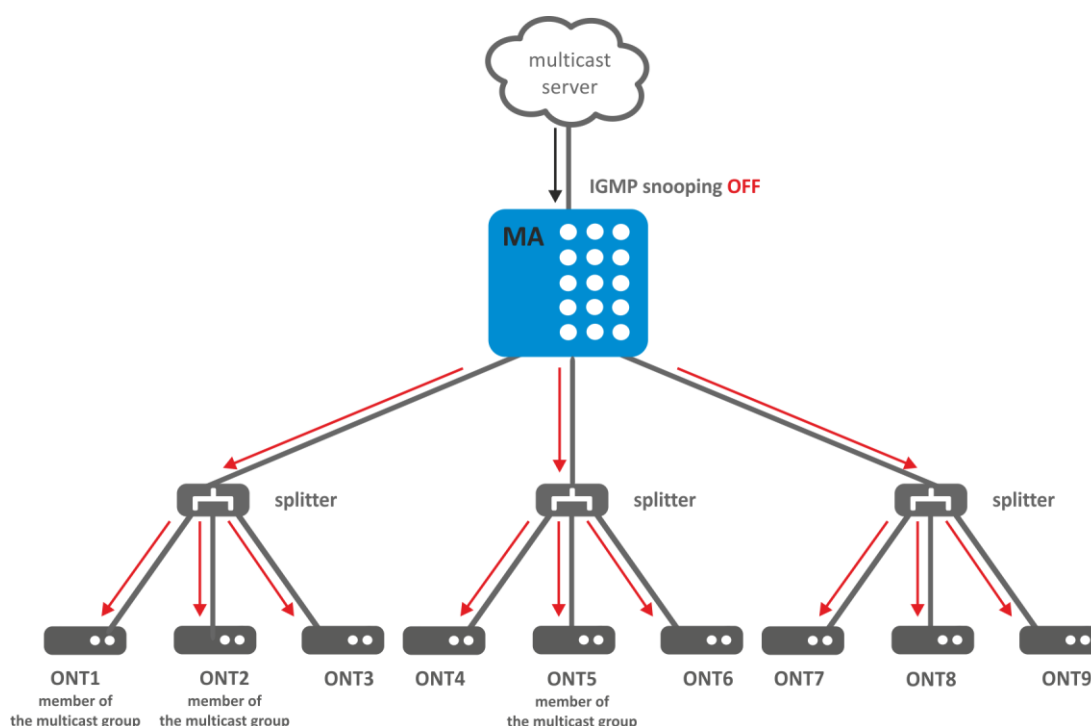


Fig. 27—IGMP Snooping Is Disabled

Figure 27 shows multicasting of IGMP traffic regardless of whether an end host needs the traffic or not.

When IGMP snooping becomes enabled, the multicasting situation changes as follows: the switch will analyse all IGMP packets between connected devices and the routers the multicast traffic comes from. When the switch receives a consumer's IGMP request for connection to a multicast group, it adds the port the consumer is connected to into the group. And vice versa, having received a request for leaving a group, the switch removes the corresponding port from the group.

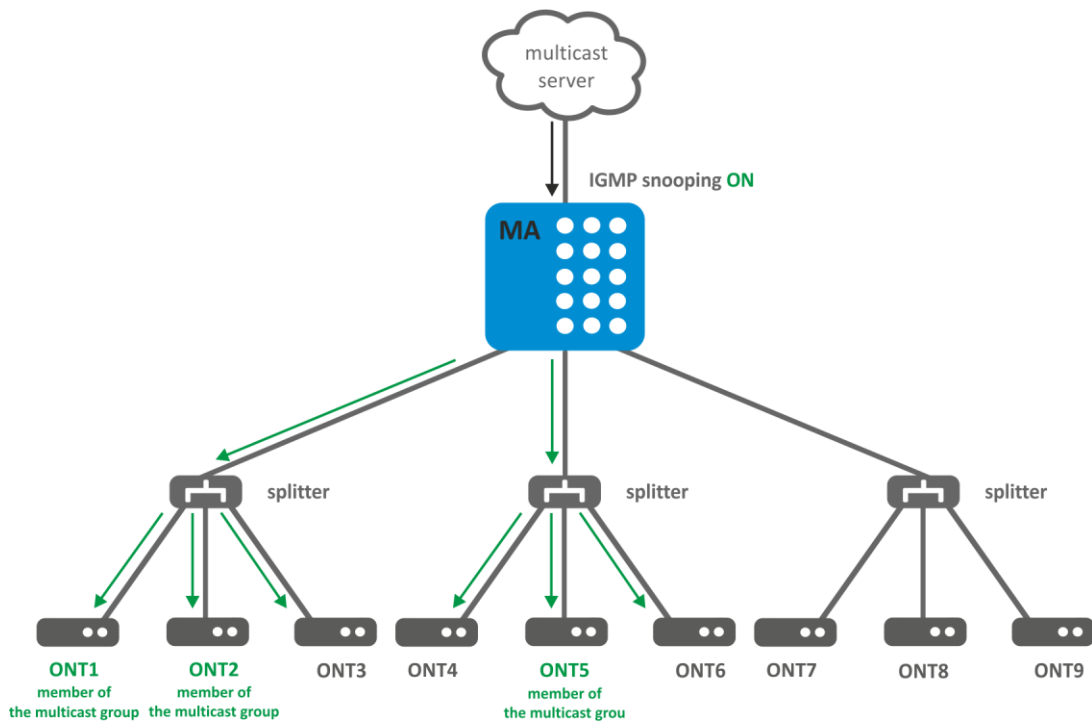


Fig. 28—IGMP Snooping Is Enabled

As you may see from Fig. 28, access node with enabled IGMP snooping translates multicast traffic only to those trees, that have sent the IGMP group connection request.

IGMP proxy is an IGMP client and group router at the same time (IGMP router). On the one hand, proxy requests an upstream router for group channels; on the other hand, it receives join/leave requests from hosts and replicates upstream traffic to the corresponding interfaces.

MLD protocol in IPv6 is similar to IGMP in IPv4, thus above information is relevant to MLD protocol too.

23.2 Multicast Configuration

Step 1. Enable IGMP snooping with the **ip igmp snooping enable** command:

```
ma4000(vlan-100)# ip igmp snooping enable
```

Step 2. Configure IGMP protocol settings for a specific slot:

```
ma4000(vlan-100)# ip igmp slot 0 query-interval 100
ma4000(vlan-100)# ip igmp slot 0 robustness 3
ma4000(vlan-100)# ip igmp slot 0 query-response-interval 125
ma4000(vlan-100)# ip igmp slot 0 last-member-query-interval 25
```

Step 3. Enable *fast-leave* feature, if necessary:

```
ma4000(vlan-100)# ip igmp snooping querier fast-leave
```

Step 4. Enable *Querier* for the specific VLAN, if necessary:

```
ma4000(vlan-100)# ip igmp snooping querier enable
```

Step 5. Define processing policy for the unrequested multicast traffic:

```
ma4000(vlan-100)# exit
ma4000(config)# ip igmp unregistered ip4-mc drop
```

Step 6. If necessary, enable *IGMP proxy*:

```
ma4000(config)# ip igmp proxy report pp4x enable
```

Step 7. Define the rules for proxying from one VLAN into another. Pass the group range, source vlan, and destination vlan as parameters.

```
ma4000(config)# ip igmp proxy report pp4x range 224.0.0.0 239.255.255.255 from
100 to 98
```

Step 8. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

23.3 IPv6 Multicast Configuration

Step 1. Enable MLD snooping by **ip mld snooping enable** command:

```
ma4000(vlan-100)# ipv6 igmp snooping enable
```

Step 2. Configure the parameters for MLD protocol for the specific slot:

```
ma4000(vlan-100)# ipv6 mld slot 0 query-interval 100
ma4000(vlan-100)# ipv6 mld slot 0 robustness 3
ma4000(vlan-100)# ipv6 mld slot 0 query-response-interval 125
ma4000(vlan-100)# ipv6 mld slot 0 last-member-query-interval 25
```

Step 3. If necessary, activate *fast-leave* function:

```
ma4000(vlan-100)# ipv6 mld snooping querier fast-leave
```

Step 4. If necessary, involve *Querier* in the specific VLAN:

```
ma4000(vlan-100)# ipv6 mld snooping querier enable
```

Step 5. Define processing policy of required multicast traffic:

```
ma4000(vlan-100)# exit
ma4000(config)# ipv6 mld unregistered ip6-mc drop
```

Step 6. Activate *MLD proxy* if necessary:

```
ma4000(config)# ipv6 mld proxy report enable
```

Step 7. Define rules for proxying between VLANs. As an argument, transmit a range of groups, vlan-source and vlan-receiver.

```
ma4000(config)# ipv6 mld proxy report range ff15:: ff15::ffff from all to 30
```

Step 8. Apply the configuration, using **commit** command.

```
ma4000(config)# do commit
```

24 DHCP RELAY AGENT CONFIGURATION

24.1 Introduction

This Chapter describes configuration of DHCP Relay Agent in the terminal.

DHCP Relay Agent is used to provide a DHCP server with additional information about a received DHCP request. This may include information about the access node running DHCP Relay Agent as well as information about the ONT which sent the DHCP request. DHCP packets are modified by interception and further processing in access node CPU.

The DHCP server identifies the ONT by analyzing DHCP option 82 and DHCPv6 options 37 and 38. DHCP Relay Agent allows the option to be both transparently transmitted from ONT as well as formed and rewritten according to a specified format. DHCP option 82 is especially useful for a network which has no private VLANs dedicated for each user.

DHCP Relay Agent supports configurable formats for both Circuit ID and Remote ID. The suboptions format is configured with the help of the tokens listed in Table 18. DHCPv6 Relay Agent supports adjustable format for Interface ID and Remote ID suboptions. The configuration of suboption format is performed by using tokens represented in Table 19. The placeholders will be replaced with corresponding values, while the rest of the words will be passed as is.

Table 18—DHCP Option 82 Tokens

%HOSTNAME%	The access node network name
%SLOTID %	The number of MA4000 slot
%MNGIP%	The access node IP address
%CHANNELID%	ID of the OLT channel the DHCP request arrived from
%ONTID%	ID of the ONT which sent the DHCP request
%PONSERIAL%	Serial number of the ONT which sent the DHCP request
%GEMID%	ID of the GEM port where the DHCP request arrived
%VLAN0%	External VID
%VLAN1%	Internal VID
%MAC%	MAC address of the ONT which sent the request
%OPT60%	DHCP option 60 received from the ONT
%OPT82 CID%	Circuit ID received from the ONT
%OPT82 RID%	Remote ID received from the ONT
%DESCR%	ONT description

Table 19 – DHCPv6 option 37 and 38 Tokens

%HOSTNAME%	The access node network name
%MNGIP%	The access node IP address
%GPON-PORT%	The number of PON port from which DHCP request has been received
%ONTID%	ONT identifier that sent the DHCP request
%PONSERIAL%	Serial number of ONT that sent the DHCP request
%GEMID%	The number of GEM port which received the DHCP request
%VLAN0%	External VID
%VLAN1%	Internal VID
%MAC%	MAC address of ONT from which the request has been received

%SLOTID%	The number of MA4000 slot
%DESCR%	Description of ONT

In addition to DHCP option, DHCP Relay Agent has some more functions related to network security. It provides protection from DoS attacks by setting a threshold for intensity of DHCP messages which are received from ONT. Exceeding the threshold blocks DHCP requests. The blocking time can be configured.

It also protects from illegal DHCP servers by controlling the source IP address of DHCP responses. Transmitted are only the DHCP responses which arrived from IP addresses of trusted DHCP servers.

24.2 DHCP Relay Agent Profiles Management

A set of profiles is used for DHCP Relay Agent configuration. All VLANs use profile *dhcp-ra-00* by default.

The configuration is flexible as it allows DHCP profiles to be assigned not only to a slot MA4000, but separately to each VLAN as well. To assign a profile, the following steps should be taken.

Step 1. Assign the default profile for all VLANs with the help of the **slot <id> profile dhcp-ra** command.

```
ma4000# configure terminal
ma4000(config)# slot 0 profile dhcp-ra dhcp-ra-00
```

Step 2. Create a new DHCP Relay Agent profile with the help of the **profile dhcp-ra** command, if necessary. Pass profile name as a parameter.

```
ma4000(config)# profile dhcp-ra dhcp-ra-01
ma4000(config-dhcp-ra) ("dhcp-ra-01")# exit
```

Step 3. Assign the newly created profile to the selected VLAN with the **slot <id> profile dhcp-ra** command. As a parameter, pass the profile name and VLAN ID.

```
ma4000(config)# slot 0 profile dhcp-ra dhcp-ra-01 vlan 100
```

Step 4. Check the changes by using the **show slot <id> gpon olt configuration** command.

```
ma4000(config) do show slot 0 gpon olt configuration
Profile pppoe-ia:                pppoe-ia-00          OLT Profile PPPoE
Intermediate Agent 0
Profile dhcp-ra:                 dhcp-ra-00           OLT Profile DHCP
Relay Agent 0
Profile dhcp-ra per VLAN 100 [0]:
Profile:                        dhcp-ra-01           OLT Profile DHCP
Relay Agent 1
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config)# do commit
```



To apply the changes, OLT should be reconfigured.

24.3 DHCP Relay Agent Profiles Configuration

Step 1. Switch to the corresponding DHCP Relay Agent profile.

```
ma4000(config)# profile dhcp-ra dhcp-ra-01
```

Step 2. Enable DHCP traffic processing with the enable command.

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# enable
```

Step 3. Enable insert/overwrite of DHCP option 82 with the help of the **overwrite-option82** command if needed.

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# overwrite-option82
```

Step 4. Specify the DHCP option 82 format with the help of the **overwrite-option82 circuit-id** and **overwrite-option82 remote-id** commands if needed. A list of possible tokens is given in [Table 18](#).

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# overwrite-option82 circuit-id "%HOSTNAME%
%MAC% %OPT82_CID%"
ma4000(config-dhcp-ra) ("dhcp-ra-01")# overwrite-option82 remote-id
"%OPT82_RID%"
```

Step 5. Enable DoS attack protection with the help of the **dos-block** command if needed. Specify the threshold for DHCP queries intensity in seconds which will block the queries when exceeded. Use the **dos-block packet-limit** command for it. Use the **dos-block block-time** command to specify the blocking time in seconds.

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# dos-block
ma4000(config-dhcp-ra) ("dhcp-ra-01")# dos-block packet-limit 200
ma4000(config-dhcp-ra) ("dhcp-ra-01")# dos-block block-time 300
```

Step 6. Set a list of trusted DHCP servers with the help of the **trusted- primary** and **trusted-secondary** commands. Specify a response timeout for DHCP servers by using the **trusted-timeout** command. Activate filters with the help of the **trusted** command.

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# trusted primary 10.0.0.1
ma4000(config-dhcp-ra) ("dhcp-ra-01")# trusted secondary 10.0.0.2
ma4000(config-dhcp-ra) ("dhcp-ra-01")# trusted timeout 200
ma4000(config-dhcp-ra) ("dhcp-ra-01")# trusted
```

Step 7. Apply the changes by using the **commit** command.

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# do commit
```



To apply the changes, OLT should be reconfigured.

24.4 DHCPv6 Relay Agent profiles management

DHCPv6 Relay Agent configuration is performed via profiles system. By default, dhcp-ra-00 profile is used for all VLANs.

The flexibility of configuration provides opportunity to assign DHCPv6 profiles not only for MA4000 slot, but for specified VLAN individually. The assignment is implemented in several steps.

Step 1. Assign a profile by default using **slot <id> profile dhcpv6-ra** command for all VLANs:

```
ma4000# configure terminal
ma4000(config)# slot 0 profile dhcpv6-ra dhcpv6-ra-00
```

Step 2. If necessary, create new *DHCPv6 Relay Agent* profile by using **profile dhcpv6-ra** command. As a parameter, define profile's name:

```
ma4000(config)# profile dhcpv6-ra dhcpv6-ra-01
ma4000(config-dhcpv6-ra) ("dhcpv6-ra-01")# exit
```

Step 3. If necessary, assign the created profile on selected VLAN, using **slot <id> profile dhcpv6-ra** command. As parameters, define profile's name and VLAN ID:

```
ma4000(config)# slot 0 profile dhcpv6-ra dhcpv6-ra-01 vlan 100
```

Step 4. Check the changes by **show slot <id> gpon olt configuration** command.

```
ma4000# show slot 1 gpon olt configuration
Profile pppoe-ia:                                pppoe-ia-00      OLT
Profile PPPoE Intermediate Agent 0
Profile dhcp-ra:                                dhcp-ra-00      OLT
Profile DHCP Relay Agent 0
Profile dhcp-ra per VLAN:                        <list is empty>
Profile dhcpv6-ra per VLAN:                      <list is empty>
Profile dhcpv6-ra:                                dhcpv6-ra-00    OLT
Profile DHCPv6 Relay Agent 0
```

Step 5. Apply the changes, using **commit** command:

```
ma4000(config)# do commit
```

24.5 DHCPv6 Relay Agent profiles configuration

Step 1. Go to a needed DHCP Relay Agent profile:

```
ma4000(config)# profile dhcpv6-ra dhcpv6-ra-01
```

Step 2. Enable DHCP traffic processing, using **enable** command:

```
ma4000(config-dhcpv6-ra) ("dhcpv6-ra-01")# enable
```

Step 3. If necessary, enable adding of DHCPv6 option 37 and 38 by **add-suboptions** command:

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# add-suboptions
```

Step 4. If necessary, define DHCPv6 option 37 and 38 formats, using **add-remote-id** and **add-interface-id** commands. The list of tokens is represented in Table 19.

```
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# add-interface-id "%PONSERIAL%"
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# add-remote-id "%OPT82_RID%"
```

Step 5. If necessary, activate protection against DoS attacks, using **dos-block** command. Set the threshold of DHCP request rate. If the threshold is exceeded, DHCP requests transmissions will be blocked by **dos-block packet-limit** command. Define the time of blocking in seconds, using **dos-block block-time** command:

```
ma4000(config-dhcpv6-ra) ("dhcpv6-ra-01")# dos-block
ma4000(config-dhcpv6-ra) ("dhcpv6-ra-01")# dos-block packet-limit 200
ma4000(config-dhcpv6-ra) ("dhcpv6-ra-01")# dos-block block-time 300
```

Step 6. Configure a list of trusted DHCP servers by **trusted primary** and **trusted secondary** commands. Define the timeout for DHCP servers by **trusted timeout** command. Activate filtration mechanism by **trusted** command:

```
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# trusted primary 1010::1
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# trusted secondary 1010::2
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# trusted timeout 200
ma4000(config-dhcpv6-ra) ("dhcp-rav6-01")# trusted
```

Step 7. Apply the changes, using **commit** command:

```
ma4000(config-dhcp-ra) ("dhcp-ra-01")# do commit
```



To apply the changes, OLT should be reconfigured.

24.6 DHCP Broadcast-to-Unicast Relay Agent Configuration

To reduce the broadcast traffic and avoid answers of illegal DHCP-servers there is an ability to use unicast messages to interact with specified DHCP-server.

Step 1. Create L3 interface: define IP address on VLAN in which customer devices are located, using **ip interface** command (only for single-tag service).

```
ma4000(config)# vlan 2000
ma4000(vlan-2000)# ip interface 10.10.10.10/32
```

Step 2. Create interface-vlan into vlan which is used for uplink to DHCP-server.

```
ma4000(config)# vlan 1209
ma4000(vlan-1209)# ip interface 192.168.209.240/24
```

Step 3. Specify DHCP server address used in unicast packets. In case the DHCP-server is located after the router, we have to use static route to this network.

```
ma4000(vlan-1209)# relay 192.168.56.1
ma4000(config)# ip route allow 192.168.56.0/24 192.168.209.5
```

25 PPPOE INTERMEDIATE AGENT CONFIGURATION

25.1 Introduction

This Chapter describes configuration of PPPoE Intermediate Agent of the access node.

PPPoE Intermediate Agent is used to provide BRAS with additional information about a received PADI request. This may include information about the terminal running PPPoE Intermediate Agent as well as information about the ONT which sent the PADI request. PADI packets are modified by interception and further processing in access node CPU.

BRAS analyses vendor specific tag and identifies the ONT. PPPoE Intermediate Agent forms or rewrites a vendor specific tag using a specified format. Vendor specific tags are especially useful for a network which has no private VLANs dedicated for each user.

PPPoE Intermediate Agent supports configurable formats for Circuit ID and Remote ID. The suboptions format is configured with the help of the tokens listed in Table 20. The placeholders will be replaced with corresponding values, while the rest of the words will be passed as is.

Table 20—Vendor Specific Tag Tokens

%HOSTNAME%	The access node network name
%SLOTID%	Slot number MA4000
%MNGIP%	The access node IP address
%CHANNELID%	ID of the OLT channel the PADI request arrived from
%ONTID%	ID of the ONT which sent the PADI request
%PONSERIAL%	Serial number of ONT that sent DHCP request
%GEMID%	ID of the GEM port where the PADI request arrived
%VLAN0%	External VID
%VLAN1%	Internal VID
%MAC%	MAC address of the ONT which sent the request
%DESCR%	First 20 symbols from ONT configuration description.

In addition to vendor specific tag support, PPPoE Intermediate Agent has some more functions related to network security. It provides protection from DoS attacks by setting a threshold for intensity of PADI messages which are received from ONT. Exceeding the threshold blocks PADI requests. The blocking time can be configured.

PPPoE Intermediate Agent also limits the number of simultaneous PPPoE sessions. The restriction can be set for both the total number of access node sessions and for every ONT separately.

25.2 PPPoE Intermediate Agent Profiles Configuration

To configure a PPPoE Intermediate Agent profile:

Step 1. Switch to the corresponding PPPoE Intermediate Agent profile.

```
ma4000# configure terminal
```

```
ma4000(config)# profile pppoe-ia pppoe-ia-00
ma4000(config-pppoe-ia) ("pppoe-ia-00") #
```

Step 2. Enable PPPoE traffic processing with the **enabled** command.

```
ma4000(config-pppoe-ia) ("pppoe-ia-00") # enable
```

Step 3. Specify the vendor specific tag format with the help of the **format circuit-id** and **format remote-id** commands. A list of possible tokens is given in Table 20.

```
ma4000(config-pppoe-ia) ("pppoe-ia-00") # format circuit-id "%HOSTNAME%"
ma4000(config-pppoe-ia) ("pppoe-ia-00") # format remote-id "%GEMID%"
```

Step 4. Enable DoS attack protection with the help of the **dos-block** command if needed. Specify the threshold for PADI queries intensity in seconds which will block the queries when exceeded. Use the **dos-block packet limit** command for it. Use the **dos-block block-time** command to specify the blocking time in seconds.

```
ma4000(config-pppoe-ia) ("pppoe-ia-00") # dos-block
ma4000(config-pppoe-ia) ("pppoe-ia-00") # dos-block packet-limit 200
ma4000(config-pppoe-ia) ("pppoe-ia-00") # dos-block block-time 300
```

Step 5. Set the limits of PPPoE sessions by using the **sessions limit** command.

```
ma4000(config-pppoe-ia) ("pppoe-ia-00") # sessions-limit 128 per-user 2
```

Step 6. Apply the changes by using the **do commit** command.

```
ma4000(config-pppoe-ia) ("pppoe-ia-00") # do commit
```



To apply the changes, OLT should be reconfigured.

26 IP SOURCE GUARD CONFIGURATION

26.1 Introduction

IP Source-Guard allows limiting unauthorized using of IP addresses (by binding IP and MAC addresses of a source to a specific service on a specific ONT). There are two operation modes:

- Static. You need to strictly define correspondence of MAC and IP addresses of a client device for transmitting traffic from the client.
- Dynamic. IP address is obtained via DHCP. Since customer device exchange data with DHCP server, DHCP Snooping table is formed on the OLT. The table contains correspondence of MAC-IP-GEM port and information on lease time. Only the packets with source MAC and source IP fields matching the records in the DHCP snooping table are passed from the client. To support client equipment with static IP addresses, static entries can be created in the dynamic mode.



To enable the IP Source Guard functions, enable DHCP-RA. For more information on DHCP-RA, see Chapter 24.



These functions are not supported in Model 1 (for more information about models, see Chapter 27).



When IP Source Guard is enabled, any non-IP traffic is forbidden.

26.2 IP Source Guard configuration

Step 1. Go to **configure** view.

```
ma4000# configure terminal
```

Step 2. Enable IP Source-Guard and set the mode.

```
ma4000(config)# ip source-guard enable
ma4000(config)# ip source-guard mode dynamic
```

Step 3. Apply the changes by **do commit** command.

```
ma4000(config)# do commit
```



Automatic reconfiguration of OLT is performed after enabling/disabling/changing the IPSG mode.

For adding of static bindings, use the following command:

```
ma4000(config)# ip source-guard bind ip <IP> mac <MAC> interface-ont <ONT> service
<NUM>
```

Where:

- IP – IP address of client equipment in X.X.X.X format,
- MAC – MAC address of client equipment in XX:XX:XX:XX:XX:XX format,
- ONT – ONT identifier in SLOT_ID/CNANNEL_ID/ONT_ID format,
- NUM – ONT service number, through which traffic with specific addresses will be transmitted, from 0 to 7.

The negative command **no** is used for IP Source Guard disabling and removing of static bindings:

```
ma4000(config)# no ip source-guard enable
ma4000(config)# no ip source-guard bind
ma4000(config)# no ip source-guard bind ip <IP>
```

The **show** command is used for viewing information on state, mode and static bindings:

```
ma4000# show slot 1 ip source-guard
IP Source Guard:
  Enabled: true
  Mode: dynamic
  Bind [0]:
    Ip: 192.168.200.90
    Mac: 00:22:B0:50:59:71
    Interface-ont: 1/0/4
```

Service:	2
----------	---

PART IV

ONT CONFIGURATION

27 SERVICE MODELS

This Chapter considers main terms and classification of service models.

27.1 Introduction

In general, a service model is based on a method which describes how the services are provided: "VLAN for Subscriber" or "VLAN for Service". The "VLAN for Service" architecture means that a service VLAN (S-VLAN) is used to provide all users with a certain service. The "VLAN for Subscriber" architecture, in its turn, implies that a client VLAN (C-VLAN) is used to provide a user with multiple services. These methods are often combined in practice and form a hybrid model which uses S-VLAN and C-VLAN simultaneously.

27.1.1 "VLAN for Subscriber" Architecture

A separate VLAN is used for each subscriber in the C-VLAN model. A dedicated C-VLAN is used to provide services to each user between OLT and service routers. Service GEM ports are created for every OLT service between ONT and OLT. When a service request is generated upstream, records are added to the MAC table in OLT according to C-VLAN. In case of downstream traffic, a corresponding GEM port is determined for a definite service according to the MAC table in OLT.

If destination address of downstream transmission is not known (broadcast or unknown unicast), i. e. the GEM port cannot be determined, two options are available:

- transmission through a dedicated broadcast GEM port;
- transmission to all GEM ports which correspond to the services provided to the subscriber.

The destination address, in case it is unknown (broadcast or unknown unicast), will be determined based on the method implemented in a definite service model.

The architecture of this service model is shown in Fig. 29.

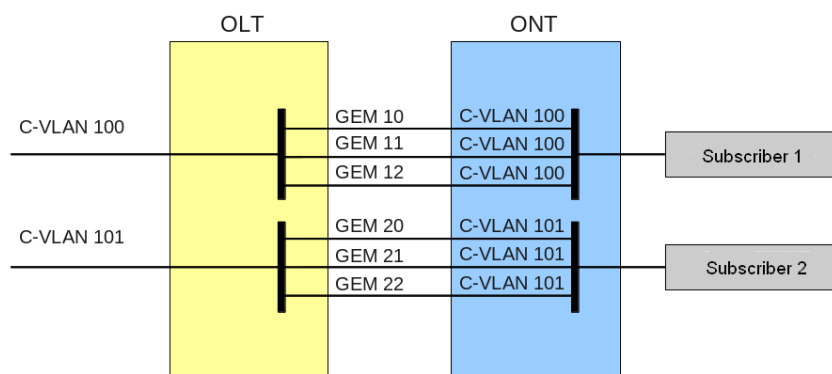


Fig. 29—"VLAN for Subscriber" Service Model Architecture

27.1.2 "VLAN for Service" Architecture

S-VLAN model has a separate VLAN for every service. Consider its operation on an example of an abstract S-VLAN 100 service.

S-VLAN 100 is used between OLT and service routers that is global for all subscribers in terms of this service. When a service request is generated upstream, records are added to the MAC table in OLT according to S-VLAN and subscriber's MAC address. In case of downstream traffic, a corresponding subscriber of the service is determined based on the MAC table.

If destination address of downstream transmission is not known (broadcast or unknown unicast), i. e. the GEM port can not be determined, two options are possible:

- transmission through a dedicated broadcast GEM port (traffic is transmitted to all subscribers);
- transmission to every subscriber through a GEM port corresponding to the service.

The GEM port, in case it is unknown (broadcast or unknown unicast), will be determined based on the method implemented in a definite service model.

The architecture of this service model is shown in Fig. 30.

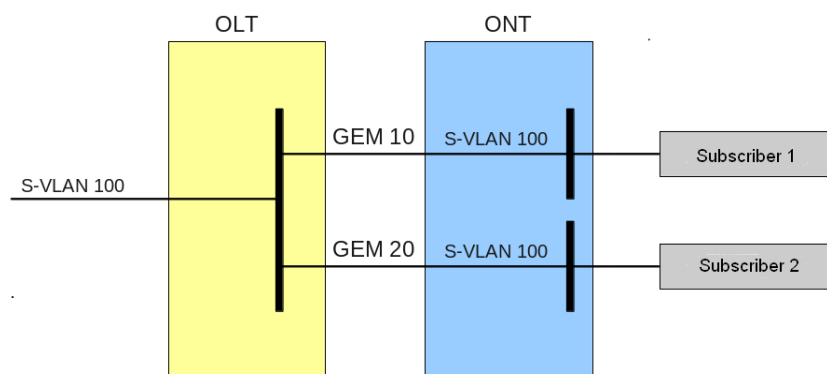


Fig. 30—"VLAN for Service" Service Model Architecture

27.2 Operating Principle

The "configuration model" concept is used for implementation of different service models of the access node. A configuration model defines general principles for data communication channelling for both OLT and ONT.

- Model 1 is an implementation of the "VLAN for Subscriber" service model. The model does not have dedicated broadcast GEM ports, and uses U-VLAN on the ONT side.
- Model 2 is an implementation of the "VLAN for Subscriber" service model. The model differs from model 1 by using a dedicated broadcast GEM port and C-VLAN on the subscriber's side.
- As opposed to the first two models, model 3 is an implementation of the "VLAN for Service" service model. The model uses a dedicated broadcast GEM port.

Table 21—Service Models

	VLAN for Service	VLAN for Subscriber	Broadcast to Unicast GEM	Dedicated Broadcast GEM
Model 1	-	+	+	-
Model 2	+	-	-	+
Model 3	+	-	-	+

27.2.1 Model 1

Consider a model 1 implementation example. The chart of this service model is shown in Fig. 31.

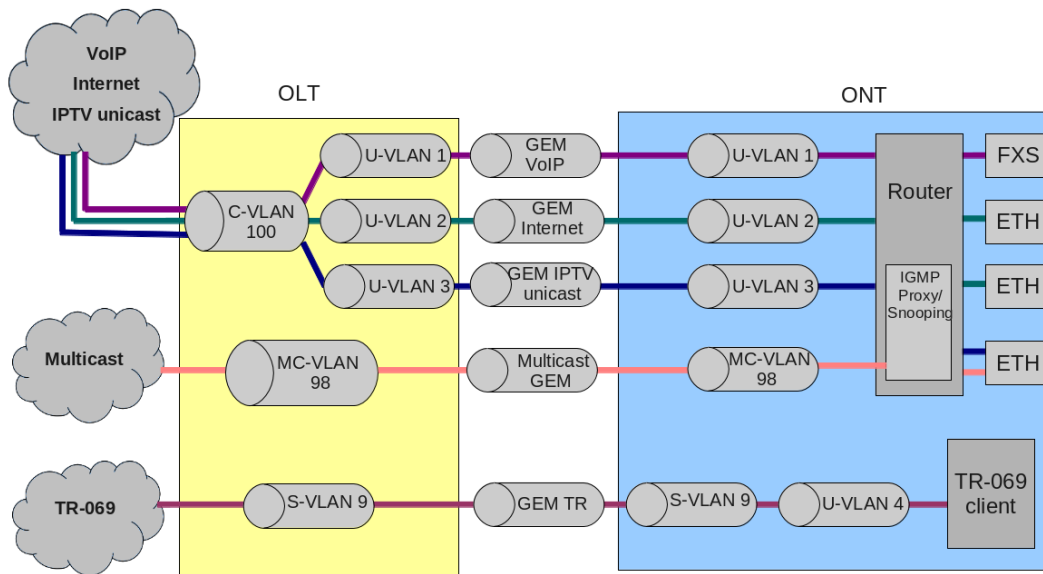


Fig. 31—Service Model 1 Chart

A C-VLAN is used between ONT and service routers (BRAS, VoIP SR) that encapsulate services for one subscriber (one ONT), such as VoIP, Internet, and IPTV unicast. An S-VLAN that is global for all subscribers (ONTs) is used for the TR-69 management service. Corresponding GEM ports are created for every OLT service between ONT and OLT. A dedicated MC-VLAN is used for multicast transmissions.

OLT casts C-VLAN (for VoIP, Internet, and IPTV unicast) or S-VLAN (for TR-069) for every service into a corresponding U-VLAN. ONT associates the U-VLAN with corresponding ONT interfaces or program modules. For example, a TR-069 service is associated with a TR-69 client with the help of a corresponding interface. VoIP, Internet, and IPTV unicast services can operate in the "router" or "bridge" modes depending on ONT configuration. The chart shows all services configured in the "router" mode.

Broadcast and unknown unicast traffic is transmitted in this model by replicating a corresponding packet (broadcast or unknown unicast) to OLT. C-VLAN replicates services to all associated GEM ports and at the same time translates data to corresponding U-VLAN for each service. TR-069 service is replicated between corresponding GEM ports of all subscribers (ONT). Thus, the model implements "VLAN for Subscriber" for VoIP, Internet, and IPTV unicast services, but uses "VLAN for Service" for TR-069 service.

27.2.2 Model 2

Consider a model 2 implementation example. The chart of this service model is shown in Fig. 32.

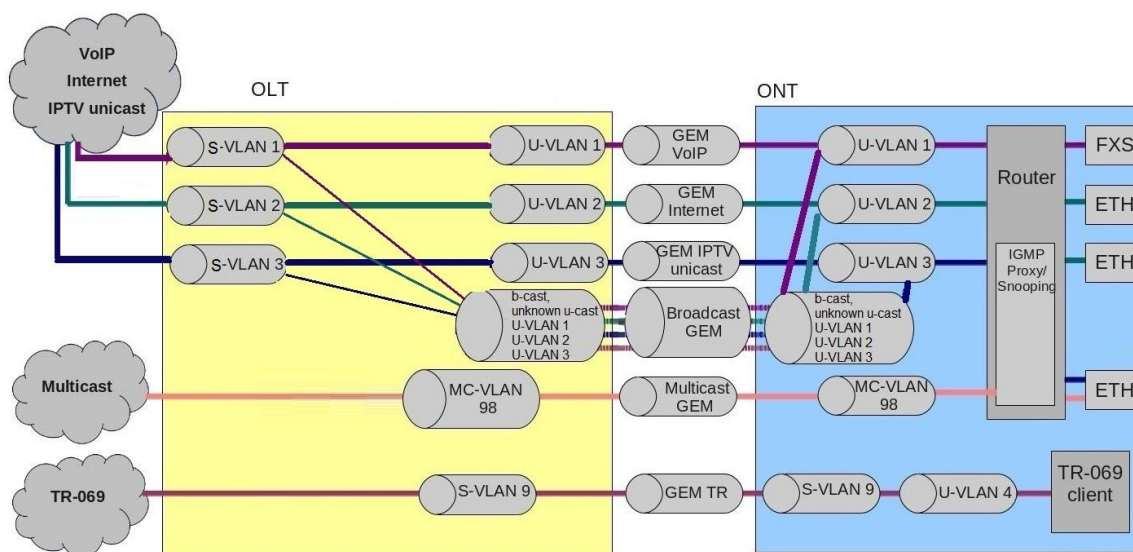


Fig. 32—Service Model 2 Chart

A S-VLAN is used between ONT and service routers (BRAS, VoIP SR) that encapsulate services for one subscriber (one ONT), such as VoIP, Internet, and IPTV unicast. An S-VLAN that is global for all subscribers (ONTs) is used for the TR-069 management service. Corresponding GEM ports are created for every OLT service by LTP-8X between ONT and OLT. A dedicated MC-VLAN is used for multicast transmissions.

VoIP, Internet, and IPTV unicast services are associated with C-VLAN in ONT. The TR-069 service is associated with S-VLAN in ONT. ONT casts C-VLAN (for VoIP, Internet, IPTV unicast) or S-VLAN (for TR-069) for every service into a corresponding U-VLAN. ONT associates the U-VLAN with corresponding ONT interfaces or program modules. For example, a TR-069 service is associated with a TR-069 client with the help of a corresponding interface. VoIP, Internet, and IPTV unicast services can operate in the "router" or "bridge" modes depending on ONT configuration. The chart shows all services configured in the "router" mode.

All broadcast and unknown unicast traffic is redirected to a dedicated broadcast GEM port in this model. Broadcast and unknown unicast packets are sent to C-VLAN (for VoIP, Internet, and IPTV unicast services) in ONT. These packets are replicated for all services in ONT with simultaneous transmission to U-VLAN. Broadcast and unknown unicast packets of the TR-069 service are sent to S-VLAN in ONT and then are transmitted to U-VLAN.

In general, the model is similar to model 3 except the one thing: transmission of C-VLAN to U-VLAN is performed on the OLT side; VoIP, Internet, and IPTV unicast traffic comes in U-VLAN to ONT.

Thus, the model implements "VLAN for Service" for VoIP, Internet, and IPTV unicast services and TR-069 service.

27.2.3 Model 3

Consider a model 3 implementation 3. The chart of this service model is shown in Fig. 33.

Dedicated S-VLANs are used between OLT and service routers (BRAS, VoIP SR) for each of the following services: VoIP, Internet, IPTV unicast, and TR-069. These S-VLAN are global for all subscribers (ONT). Corresponding GEM ports are created for every OLT service between ONT and OLT. A dedicated MC-VLAN is used for multicast transmissions.

VoIP, Internet, and IPTV, and TR-069 unicast services are associated with S-VLAN in ONT. ONT transmits S-VLAN into a corresponding U-VLAN for each service. ONT associates the U-VLAN with corresponding ONT interfaces or program modules. For example, a TR-069 service is associated with a TR-069 client with the help of a corresponding interface. VoIP, Internet, and IPTV unicast services can operate in the "router" or "bridge" modes depending on ONT configuration. The chart shows all services configured in the "router" mode.

All broadcast and unknown unicast traffic is redirected to a dedicated broadcast GEM port in this model. Broadcast and unknown unicast packets come to S-VLAN in ONT. These packets are transmitted into the corresponding U-VLANs on the ONT side. In this case broadcast and unknown unicast are replicated neither in OLT nor in ONT since every service has a separate S-VLAN for broadcast and unknown unicast traffic.

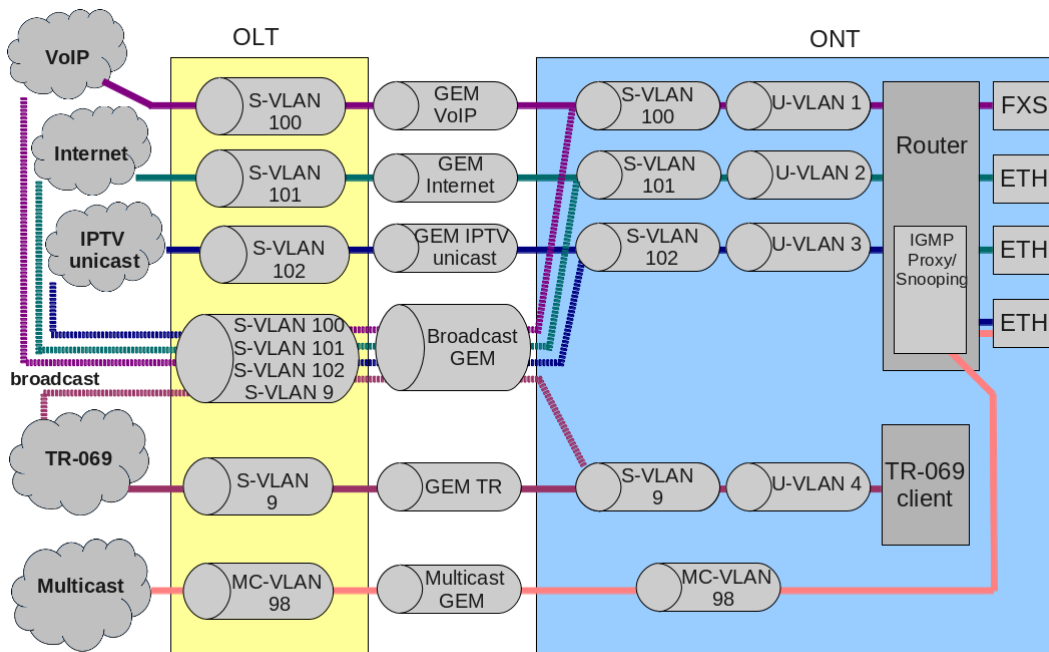


Fig. 33—Service Model 3 Chart

Thus, the model implements "VLAN for Service".

27.3 Model Configuration

Step 1. Check the current configuration with the help of the **show gpon olt general** command.

```
ma4000# show gpon olt
Block duplicated mac:          enabled
Ont block time:                5
Dhcpna shaper:                 100
Datapath:
  Model:                       model1
  Broadcast gem port:           4095
```

Multicast gem port:	4094
Encryption:	
Enable:	false
Key update interval:	1
ONT authentication mode:	both
Auto reconfigure ont:	true
Auto reconfigure channel:	true
Auto reconfigure olt:	true
Ont sn format:	literal

Step 2. Set model by using the **gpon olt model** command.

```
ma4000# configure terminal
ma4000(config)# gpon olt model 1
```

Step 3. Apply the changes by using the **do commit** command.

```
ma4000(config)# do commit
```

28 ONT CONFIGURATION

28.1 Introduction

This Chapter describes general principles of ONT configuration. It also defines configuration profiles.

ONT is configured with the help of a profile which defines high-level expression of data communication channels. All operations related to channel creation are performed automatically. The way the data communication channels are created depends on the selected service model (see Chapter [27 Service Models](#), page 88).

ONT configuration includes assignment of configuration profiles and specification of ONT specific parameters. Configuration profiles allow general parameters to be set for all or for a range of ONTs. Profile parameters may include, for instance, DBA settings, configuration of VLAN operations in OLT and ONT, settings of Ethernet ports in ONT. Specific ONT parameters allow each separate ONT to have its own settings specified. Such settings include, for example, GPON password, subscriber's VLAN, etc.

28.2 General Configuration Principles

Service is the key term of ONT configuration. This term completely includes a channel through which data is transferred from the interfaces located on the front panel of the terminal (see Chapter [15 Interfaces Configuration](#)) to users' ports of ONT. There are two service profiles: cross-connect and dba. The cross-connect profile creates a GEM service port, the dba profile allocates an Alloc-ID for this ONT and associates a corresponding GEM port to the Alloc-ID.

Table 22—ONT Profiles

Profile	Description
cross-connect	Defines VLAN transformation in OLT and ONT
dba	Defines upstream traffic parameters
shaping	Defines restrictions for upstream and downstream service traffic
management	Defines TR-69 management service parameters
ports	Defines user port groups in ONT as well as IGMP and multicast parameters for user ports
scripting	Allows manual configuration with the help of GPON and OMCI primitives

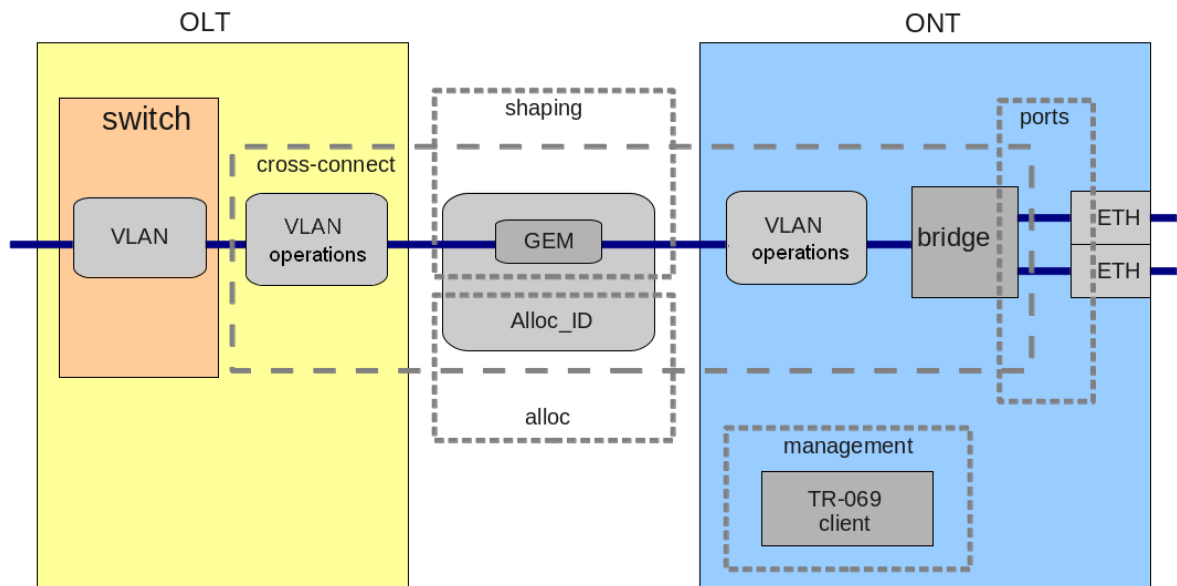


Fig. 34—ONT Scope of Operation

28.3 ONT Profiles Configuration

28.3.1 Cross-Connect Profile Configuration

Step 1. To configure a cross-connect profile, you need first to specify whether the service will be routed (transmitted through an ONT router) or bridged (use bridge connection). This can be done by changing the **model** parameter.

Step 2. Then you need to specify a service type in the **type** parameter. Some service types require the **iphost-eid** parameter to be set which allows you to choose a definite instance of IP interface in ONT.

Step 3. VLAN is configured in a cross-connect profile with the help of the following parameters: **tag-mode**, **outer-vid**, **outer-cos**, **inner-vid**, **u-vid**, and **u-cos**.

Step 4. **tag-mode** enables upstream Q-in-Q mode. **outer-vid**, **outer-cos**, and **inner-vid** specify internal and external Q-in-Q tags correspondingly. The CoS value of the internal tag is copied from the external one in this case. If the Q-in-Q mode is not used, only the **outer-vid** and **outer-cos** parameters are valid. The **u-vid** and **u-cos** parameters allow a tag to be specified which will be used on the ONT side.

Step 5. The **mac-table-entry-limit** parameter allows restriction of records number in the MAC table of OLT for this service.

Step 6. The **priority-queue** parameter allows allocation of all services of one T-CONT into queues with priorities (if ONT supports this method).

28.3.2 DBA Profile Configuration

This profile configures dynamic bandwidth allocation (DBA). These parameters allow specification of any T-CONT type described in G.984.3.

Step 1. First of all, choose a **service-class**, which will define the basic DBA algorithm.

Step 2. After that configure **status-reporting** which defines a type of ONT queues status report.

Step 3. The **fixed-bandwidth**, **guaranteed-bandwidth**, and **besteffort-bandwidth** parameters define the fixed, guaranteed, and best-effort bandwidth correspondingly.

DBA configuration is described in details in Chapter 29.

28.3.3 Shaper Profile Configuration

Configuration of this profile allows restriction of upstream and downstream services.

Step 1. Downstream restriction in OLT uses the policing algorithm. The restriction can either use one policer for all services or individual policers for each separate service. This is specified in the **one-policer** parameter. When one policer is used for all services, only **policer 0** should be specified; otherwise policers for all services should be adjusted.

Step 2. Upstream restriction in ONT uses the shaping algorithm. You can specify either a global shaper or individual shapers for unicast, multicast, and broadcast traffic (ONT functionality).

28.3.4 Ports Profile Configuration

The "ports" profile allows you to group ports in ONT. The profile also contains IGMP and multicast setting as they are separately adjusted for each port.

You can adjust up to 4 Ethernet ports and a VEIP virtual port which will serve as a link between OMCI and RG domains in ONT.

Step 1. Ethernet ports are grouped with the help of the **bridge-group** parameter. Value 0 means that the port is associated with an RG domain (router). Other values means port association with an OMCI domain, i. e. the port can be directly used in OLT to establish a data communication channel.

Step 2. IGMP and multicast configuration is described in details in Chapter [32 Multicast Configuration](#).

28.3.5 Management Profile Configuration

The management profile enables specific configuration of TR-069 management protocol, namely configuration of TR-client in ONT.

Step 1. The "enable-omci-configuration" parameter defines the TR client configuration which can be done either automatically with DHCP (all other parameters of the profile are not used in this case) or with OMCI using the profile settings.

Step 2. The "url" parameter corresponds to the address of the auto configuration server (ACS), whose access parameters are defined by the "username" and "password" parameters.

The TR-069 protocol configuration is described in details in Chapter [34 TR-069 Protocol Management Configuration](#).

28.4 ONT Configuration Procedure

Figure 35 shows steps of ONT configuration.

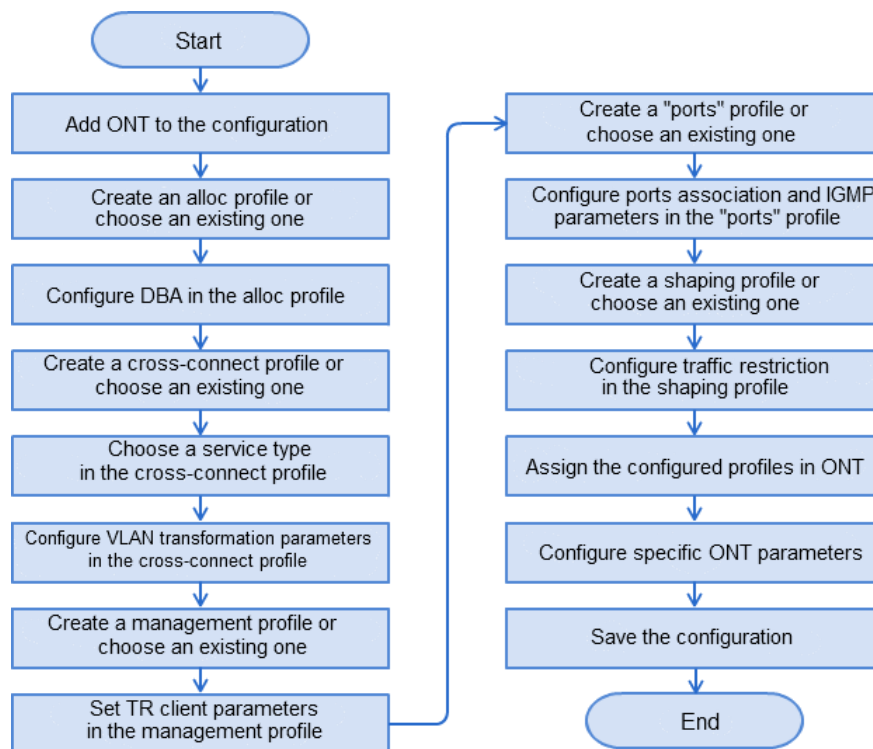


Fig. 35—ONT Configuration Procedure

Step 1. Prior to proceed to ONT configuration, add the ONT into an OLT configuration. For an ONT to be added and configured, it does not need to physically connected to OLT. You can view the list of unactivated ONTs with the help of the **show interface ont unactivated** command:

```

ma4000# show interface ont 0/0/0 unactivated

Slot 0 GPON-port 0 has no unactivated ONTs

Slot 0 total ONT count: 0
  
```

Step 2. To specify ONT settings, go to the corresponding view with the help of the **interface ont** command. Specify ONT serial number, password, or their combination.

```

ma4000# configure terminal
ma4000(config)# interface ont 0/0/0
ma4000(config)(if-ont-0/0/0)# serial ELTX5C00008C
ma4000(config)(if-ont-0/0/0)# password 0000000000
  
```

Step 3. Apply the changes by using the **do commit** command.

```

ma4000(config)(if-ont-0/0/0)# do commit
  
```

Step 4. OLT entry configuration has pre-defined ONT profiles which will be automatically assigned to ONT. View the ONT configuration with the help of the **do show interface ont 0/0/0 configuration** command.

```
ma4000(config)(if-ont-0/0/0)# do show interface ont 0/0/0 configuration
```

```
-----
[ONT0/0] configuration
-----
```

```

Description:                               ''
Status:                                     UP
Serial:                                    000000000000000000
Password:                                  ''
Fec up:                                   false
Downstream broadcast:                     true
Ber interval:                             100000
Ber update period:                        60
Rf port state:                            no change
Omci error tolerant:                      false
Service [0]:
    Profile cross connect:                 crossconnect-00    ONT Profile Cross
Connect 0
    Profile dba:                           dba-00            ONT Profile DBA 0
Service [1]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [2]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [3]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [4]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [5]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [6]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Service [7]:
    Profile cross connect:                 unassigned
    Profile dba:                           unassigned
Profile shaping:                           shaping-00        ONT Profile Shaping 0
Profile ports:                             ports-00         ONT Profile Ports 0
Profile management:                        management-00    ONT Profile Management 0
Profile scripting:                         unassigned
Custom model:                             none
Template:                                 unassigned

```

28.4.1 Model 1

Consider configuration of a data communication channel which is based on model 1 and implements "VLAN for Subscriber". Figure 36 shows a configuration of two abstract services with subscriber C-VLAN 200 and U-VLAN 10 and 11 for each service correspondingly.

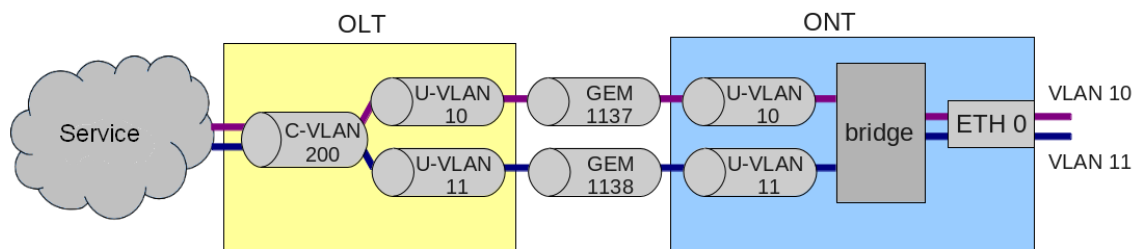


Fig. 36—Service Abstract Representation for Model 1

Step 1. Assign a service model:

```
ma4000# configure terminal
ma4000(config)# gpon olt model 1
```

Step 2. Create a Service1 cross-connect profile to configure the first service. Configure a bridged service and specify a bridged group which will be associated with an ONT port. Configure U-VLAN with the help of the **set u-vid** command (it equals 10 for the first service in this case):

```
ma4000(config)# profile cross-connect Service1
ma4000(config-cross-connect) ("Service1")# bridge
ma4000(config-cross-connect) ("Service1")# bridge group 1
ma4000(config-cross-connect) ("Service1")# user vid 10
```

Step 3. Check the changes made.

```
ma4000(config-cross-connect) ("service1")# do show profile cross-connect service1
Name:                                     'service1'
Description:                             'ONT Profile Cross Connect
1'
Model:                                    ont
Bridge group:                             1
Tag mode:                                 single-tagged
Outer vid:                                 1
Outer cos:                                 unused
Inner vid:                                 -
U vid:                                    10
U cos:                                    unused
Mac table entry limit:                    unlimited
Type:                                     general
Iphost eid:                               0
Priority queue:                           0
```

Step 4. By analogy with the described above, create another cross-connect profile (Service2) for the second service and configure it with **U-VLAN 11**:

```
ma4000(config)# profile cross-connect Service2
ma4000(config-cross-connect) ("Service2")# bridge
ma4000(config-cross-connect) ("Service2")# bridge group 1
ma4000(config-cross-connect) ("Service2")# user vid 11
```

Step 5. Check the amendments made.

```
ma4000(config-cross-connect)("service2")# do show profile cross-connect service2
  Name:                                     'service2'
  Description:                             'ONT Profile Cross Connect
2'
  Model:                                   ont
  Bridge group:                             1
  Tag mode:                               single-tagged
  Outer vid:                               1
  Outer cos:                               unused
  Inner vid:                               -
  U vid:                                   untagged
  U cos:                                   unused
  Mac table entry limit:                   unlimited
  Type:                                    general
  Iphost eid:                              0
  Priority queue:                           0
```

Step 6. Specify DBA parameters. To do this, create an dba profile and adjust the corresponding settings. We set a value of guaranteed bandwidth for this example:

```
ma4000(config)# profile dba AllServices
ma4000(config-dba)("AllServices")# bandwidth guaranteed 500
```

Step 7. Check the amends made.

```
ma4000(config-dba)("AllServices")# do show profile dba AllServices
  Name:                                     'AllServices'
  Description:                             'ONT Profile DBA 2'
  Db:
    Sla data:
      Service class:                       type5
      Status reporting:                     nsr
      Alloc size:                           0
      Alloc period:                         0
      Fixed bandwidth:                      0
      Guaranteed bandwidth:                  500
      Besteffort bandwidth:                  1244000
```

Step 8. Associate a bridge port with an ONT port. To do this, create a "ports" profile and assign value 1 to the "bridge group" parameter for the "eth 0" port:

```
ma4000(config)# profile ports Ports1
ma4000(config-ports)("Ports1")# port 0 bridge group 1
```

Step 9. Check the changes made.

```
ma4000(config-ports)("Ports1")# do show profile ports Ports1
  Name:                                     'Ports1'
  Description:                             'ONT Profile Ports 1'
  Icmp settings:
    Version:                               3
    Mode:                                   snooping
    Immediate leave:                       false
    Robustness:                             2
    Querier ip:                             0.0.0.0
    Query interval:                         125
    Query response interval:                 100
    Last member query interval:              10
    Multicast dynamic entry [0]:
      Vlan id:                               unused
```

```

        First group ip:                0.0.0.0
        Last group ip:                 0.0.0.0
    Multicast dynamic entry [1]:
        Vlan id:                       unused
        First group ip:                 0.0.0.0
        Last group ip:                 0.0.0.0
    Multicast dynamic entry [2]:
        Vlan id:                       unused
        First group ip:                 0.0.0.0
        Last group ip:                 0.0.0.0
    Multicast dynamic entry [3]:
        Vlan id:                       unused
        First group ip:                 0.0.0.0
        Last group ip:                 0.0.0.0
    Multicast dynamic entry [4]:
        Vlan id:                       unused
        First group ip:                 0.0.0.0
        Last group ip:                 0.0.0.0
    Veip:
        Multicast enable:               false
        Multicast port settings:
            Upstream igmp vid:          1
            Upstream igmp prio:         0
            Upstream igmp tag control:  pass
            Downstream multicast vid:   1
            Downstream multicast prio:  0
            Downstream multicast tag control: pass
            Max groups:                 0
            Max multicast bandwidth:    0
    Port [0]:
        Bridge group:                   1
        Spanning tree for bridge group: false
        Multicast enable:               false
        Multicast port settings:
            Upstream igmp vid:          1
            Upstream igmp prio:         0
            Upstream igmp tag control:  pass
            Downstream multicast vid:   1
            Downstream multicast prio:  0
            Downstream multicast tag control: pass
            Max groups:                 0
            Max multicast bandwidth:    0
        Shaper downstream:
            Enable:                     false
            Committed rate:              1000000
        Shaper upstream:
            Enable:                     false
            Committed rate:              1000000
    ...

```

Step 10. Assign the created profiles in ONT.

```

ma4000(config)# interface ont 0/0/0
ma4000(config)(if-ont-0/0/0)# service 0 profile dba AllServices
ma4000(config)(if-ont-0/0/0)# service 0 profile cross-connect Service1
ma4000(config)(if-ont-0/0/0)# service 1 profile dba AllServices
ma4000(config)(if-ont-0/0/0)# service 1 profile cross-connect Service2
ma4000(config)(if-ont-0/0/0)# profile ports Ports1
ma4000(config)(if-ont-0/0/0)# do show interface ont 0/0/0 configuration

-----
[ONT0/0/0] configuration
-----

Description:      ''
Status:           UP
Serial:           0000000000000000
Password:         ''

```

Fec up:	false	
Downstream broadcast:	true	
Ber interval:	100000	
Ber update period:	60	
Rf port state:	no change	
Omci error tolerant:	false	
Service [0]:		
Profile cross connect:	Service1	ONT
Profile Cross Connect 4		
Profile dba:	AllServices	ONT
Profile DBA 2		
Service [1]:		
Profile cross connect:	Service2	ONT
Profile Cross Connect 3		
Profile dba:	AllServices	ONT
Profile DBA 2		
Service [2]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Service [3]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Service [4]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Service [5]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Service [6]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Service [7]:		
Profile cross connect:	unassigned	
Profile dba:	unassigned	
Profile shaping:	shaping-00	ONT
Profile Shaping 0		
Profile ports:	Ports1	ONT
Profile Ports 1		
Profile management:	management-00	ONT
Profile Management 0		
Profile scripting:	unassigned	
Custom model:	none	
Template:	unassigned	

Step 11. "VLAN for Subscriber" requires C-VLAN to be assigned for this ONT (subscriber). Assign C-VLAN 200 for both services by using the **service <x> custom cvid** command:

ma4000(config)(if-ont-0/0/0)# service 0 custom cvid 200		
ma4000(config)(if-ont-0/0/0)# service 1 custom cvid 200		
ma4000(config)(if-ont-0/0/0)# do show interface ont 0/0/0 configuration		

[ONT0/0/0] configuration		

Description:	' '	
Status:	UP	
Serial:	0000000000000000	
Password:	' '	
Fec up:	false	
Downstream broadcast:	true	
Ber interval:	100000	
Ber update period:	60	
Rf port state:	no change	
Omci error tolerant:	false	
Service [0]:		
Profile cross connect:	Service1	ONT
Profile Cross Connect 4		

Profile dba:	AllServices	ONT
Profile DBA 2		
Custom vlan:	200	
Custom CoS:	unused	
Service [1]:		
Profile cross connect:	Service2	ONT
Profile Cross Connect 3		
Profile dba:	AllServices	ONT
Profile DBA 2		
Custom vlan:	200	
Custom CoS:	unused	
...		

Step 12. Apply the changes by using the **commit** command.

```
ma4000(config)(if-ont-0/0/0)# do commit
```

Step 13. Configure VLAN 200 in the switch view (see Chapter [13 VLAN Configuration](#)).

```
ma4000# configure terminal
ma4000(config)# vlan 200
ma4000(vlan-200)# tagged plc-front-port 0/0
ma4000(vlan-200)# tagged plc-pon-port 0/0-7
ma4000(vlan-200)# exit
ma4000(vlan-200)# do commit
```

28.4.2 Model 2

Configuration of the Model 2 is the same as for Model 3. Abstract view is represented in chapter 27.2.2.

28.4.3 Model 3

A service model which classified as model 3 implements the "VLAN for Service" principle. Fig. 37 shows an abstract service configured with S-VLAN 30.

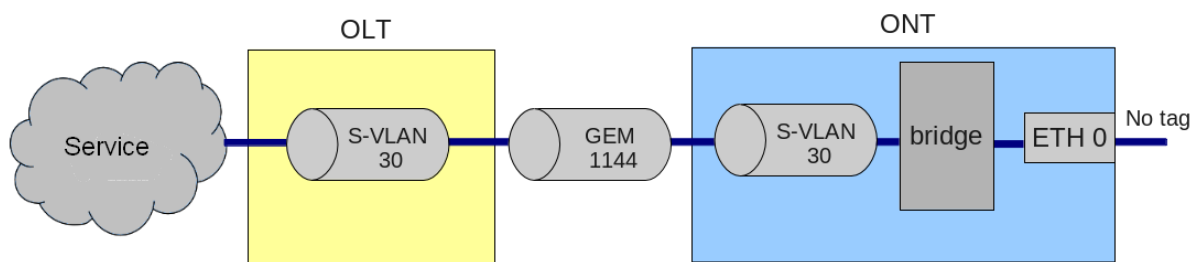


Fig. 37—Service Abstract Representation for Model 3

Step 1. Assign a service model:

```
ma4000# configure terminal
ma4000(config)# gpon olt model 3
```

Step 2. Create a Service3 cross-connect profile to configure the service. Configure a bridged service and specify the bridged group the ONT port will be associated with:


```
ma4000(config)# profile cross-connect Service3
ma4000(config-cross-connect) ("Service3")# bridge
ma4000(config-cross-connect) ("Service3")# bridge group 1
```

Step 3. To assign an S-VLAN, use the outer vid 30 command.

```
ma4000(config-cross-connect) ("Service3")# outer vid 30
```

Step 4. Specify U-VID in order to have untagged traffic coming from the ONT port.

```
ma4000(config-cross-connect) ("Service3")# user vid untagged
```

Step 5. Check the changes made.

```
ma4000(config-cross-connect) ("Service3")# do show profile cross-connect Service3
Name:                                     'Service3'
Description:                             'ONT Profile Cross Connect
3'
Model:                                    ont
Bridge group:                             1
Tag mode:                                 single-tagged
Outer vid:                                 30
Outer cos:                                 unused
Inner vid:                                 -
U vid:                                    untagged
U cos:                                    unused
Mac table entry limit:                    unlimited
Type:                                     general
Iphost eid:                               0
Priority queue:                           0
```

Step 6. Specify DBA parameters. To do this, create an dba profile and adjust the corresponding settings. We set a value of guaranteed bandwidth for this example:

```
ma4000(config)# profile dba AllServices
ma4000(config-dba) ("AllServices")# bandwidth guaranteed 500
```

Step 7. Check the changes made.

```
ma4000(config-dba) ("AllServices")# do show profile dba AllServices
Name:                                     'AllServices'
Description:                             'ONT Profile DBA 2'
Dba:
  Sla data:
    Service class:                         type5
    Status reporting:                      nsr
    Alloc size:                             0
    Alloc period:                           0
    Fixed bandwidth:                        0
    Guaranteed bandwidth:                   500
    Besteffort bandwidth:                   1244000
```

Step 8. Associate a bridge group with an ONT port. To do this, create a "ports" profile and assign value 1 to the "bridge group" parameter for the "eth 0" port.

```
ma4000(config)# profile ports Ports1
ma4000(config-ports) ("Ports1")# port 0 bridge group 1
```

Step 9. Check the changes made.

```

ma4000(config-ports)("Ports1")# do show profile ports Ports1
  Name:                                     'Ports1'
  Description:                             'ONT Profile Ports 1'
...

Port [0]:
  Bridge group:                            1
  Spanning tree for bridge group:          false
  Multicast enable:                        false
  Multicast port settings:
    Upstream igmp vid:                     1
    Upstream igmp prio:                    0
    Upstream igmp tag control:              pass
    Downstream multicast vid:               1
    Downstream multicast prio:              0
    Downstream multicast tag control:        pass
    Max groups:                             0
    Max multicast bandwidth:                0
  Shaper downstream:
    Enable:                                false
    Committed rate:                        1000000
  Shaper upstream:
    Enable:                                false
    Committed rate:                        1000000

```

Step 10. Assign the created profiles in ONT.

```

ma4000(config)# interface ont 0/0/1
ma4000(config)(if-ont-0/0/1)# service 0 profile dba AllServices
ma4000(config)(if-ont-0/0/1)# service 0 profile cross-connect Service1
ma4000(config)(if-ont-0/0/1)# profile ports Ports1
ma4000(config)(if-ont-0/0/1)# do show interface ont 0/0/1 configuration

-----
[ONT0/0/1] configuration
-----

Description:                               ''
Status:                                     UP
Serial:                                    0000000000000000
Password:                                  '0000000000'
Fec up:                                    false
Downstream broadcast:                      true
Ber interval:                              100000
Ber update period:                         60
Rf port state:                             no change
Omci error tolerant:                       false
Service [0]:
  Profile cross connect:                    Service1          ONT
Profile Cross Connect 4
  Profile dba:                              AllServices        ONT
Profile DBA 2
Service [1]:
  Profile cross connect:                    unassigned
  Profile dba:                              unassigned
Service [2]:
  Profile cross connect:                    unassigned
  Profile dba:                              unassigned
Service [3]:
  Profile cross connect:                    unassigned
  Profile dba:                              unassigned
Service [4]:
  Profile cross connect:                    unassigned
  Profile dba:                              unassigned
Service [5]:
  Profile cross connect:                    unassigned
  Profile dba:                              unassigned

```

```

Service [6]:
  Profile cross connect:      unassigned
  Profile dba:                unassigned
Service [7]:
  Profile cross connect:      unassigned
  Profile dba:                unassigned
  Profile shaping:            shaping-00      ONT
Profile Shaping 0
  Profile ports:              Ports1          ONT
Profile Ports 1
  Profile management:         management-00   ONT
Profile Management 0
  Profile scripting:          unassigned
  Custom model:               none
  Template:                   unassigned

```

Step 11. Apply the changes by using the **do commit** command.

```
ma4000(config)(if-ont-0/0/1)# do commit
```

Step 12. You will also need to configure S-VLAN 30 in the switch view (see Chapter [13 VLAN Configuration](#)).

```

ma4000# configure terminal
ma4000(config)# vlan 30
ma4000(vlan-30)# tagged plc-front-port 0/0
ma4000(vlan-30)# tagged plc-pon-port 0/0-7
ma4000(vlan-30)# exit
ma4000(vlan-30)# do commit

```

28.5 Tunnelling configuration

Simple profiles with tag-mode, single-tag and double-tag is aimed to modify traffic transmitted to gem with user vid tag or untagged into traffic with outer vid or outer:inner vid tags respectively.

The configuration of traffic tunnelling is possible on models 2 and 3. It allows extending range of possible applications of GPON on service provider networks.

The applying of profiles with 'tag-mode selective-tunnel' allows you to add a tag to received packets with specific 'user vid' tag set. Profiles with 'tag-mode tunnel' allows adding a tag to received packets with any 'user vid' tags.

Consider the following diagram and its configuration as an example:

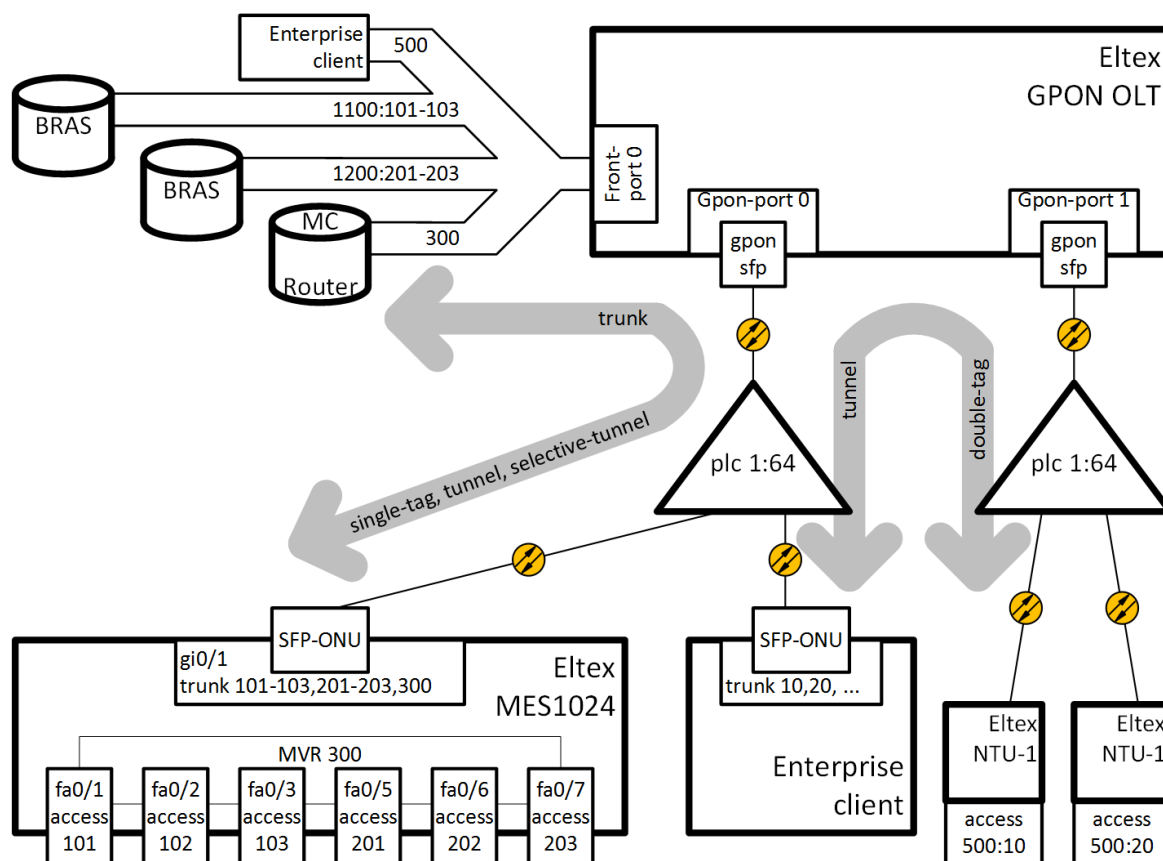


Fig. 38 - The scheme of connection

VLAN 300 (multicast) and QinQ VLAN 1100 and 1200 (the Internet) come to the uplink OLT. It is necessary to let them pass to the switch integrated in the OLT via SFP-ONU. In addition, a corporate client is connected to the splitter via SFP-ONU that sends a random set of VLANs to be passed to remote devices after removing tags of these VLANs at the ONT LAN port. To organise a tunnel for this client, VLAN 500 is selected in the operator's network.

Consider the procedure of OLT configuration for the above diagram.

Step 1. Configure the switch.

```
interface plc-pon-port 0/0
    bridging to plc-pon-port 0/1
exit
interface plc-pon-port 0/1
    bridging to plc-pon-port 0/0
exit
vlan 300
    name VLAN0300
    tagged plc-pon-port 0/0
    tagged front-port 1/0
exit
vlan 500
    name VLAN0500
    tagged plc-pon-port 0/0
    tagged plc-pon-port 0/1
    tagged front-port 1/0
exit
vlan 1100
    name VLAN1100
```

```
    tagged plc-pon-port 0/0
    tagged front-port 1/0
exit
vlan 1200
    name VLAN1200
    tagged plc-pon-port 0/0
    tagged front-port 1/0
exit
```

Step 2. Set up cross-connect profiles.

```
profile cross-connect "cc-tunnel"
bridge
bridge group "10"
tag-mode tunnel
exit
profile cross-connect "cc-selecttunnel"
bridge
bridge group "10"
tag-mode selective-tunnel
exit
profile cross-connect "cc-single"
bridge
bridge group "10"
user vid "300"
exit
profile cross-connect "cc-double"
bridge
bridge group "10"
tag-mode double-tagged
exit
```

Step 3. Set up ports profiles.

```
profile ports "bridge-10"
port 0 bridge group "10"
exit
```

Step 4. Set up address-table profile by defining VLAN used for tunnels. Assign the profile on gpon ports.

```
profile address-table "at-tunnel"
s-vlan 1100 use c-vlan
s-vlan 1200 use c-vlan
s-vlan 500 use c-vlan
exit interface gpon-port 0
profile address-table "at-tunnel"
exit
interface gpon-port 1
profile address-table "at-tunnel"
exit
```

Step 5. Set up SFP-ONU which will be used for switch connection.

```
interface ont 0/0/0
serial "454C545300000001"
service 0 profile cross-connect "cc-tunnel"
service 0 profile dba "dba-00"
service 1 profile cross-connect "cc-selecttunnel"
service 1 profile dba "dba-00"
service 2 profile cross-connect "cc-single"
service 2 profile dba "dba-00"
profile ports "bridge-10"
```

```
service 0 custom svid "1100"  
service 1 custom svid "1200"  
service 1 selective-tunnel uvid 201-203  
service 2 custom svid "300"
```

Step 6. Set up SFP-ONU which will be used for corporate client connection.

```
interface ont 0/1  
serial "454C545300000002"  
service 0 profile cross-connect "cc-tunnel"  
service 0 profile dba "dba-00"  
profile ports "bridge-10"  
service 0 custom svid "500"
```

Step 7. Set up ONT which will be used for remote offices connection.

```
interface ont 1/0  
serial "454C545800000002"  
service 0 profile cross-connect "cc-double"  
service 0 profile dba "dba-00"  
profile ports "bridge-10"  
service 0 custom cvid "10"  
service 0 custom svid "500"  
exit  
interface ont 1/1  
serial "454C545800000003"  
service 0 profile cross-connect "cc-double"  
service 0 profile dba "dba-00"  
profile ports "bridge-10"  
service 0 custom cvid "20"  
service 0 custom svid "500"
```



Tunnel and selective-tunnel services are supported only on Eltex SFP-ONU at the moment of MA4000 3.26.0 release.

The quantity of uvid processed by selective-tunnel services on a single ONT should not exceed 42.

The VLANs used for tunnel services cannot be used for other types of services within one GPON channel.

The tunnel service is the last one to be configured on the ONT, thus user-vid used by another service will not be processed by tunnel service.

The traffic transmitted with a random user-vid tag should not contain any additional 802.1q tag. Otherwise, the traffic will be rejected by a service to which user-vid tag is concerned.

It is not recommended to use untagged traffic for tunneling.

29 DBA CONFIGURATION

29.1 Introduction

This Chapter considers DBA configuration for ONT.

GPON technology implies that all ONTs of one GPON channel use common communication medium (fibre). It is necessary to provide a mechanism that will ensure data transfer from all ONTs without collisions. The mechanism is called *dynamic bandwidth allocation (DBA)* and ensures allocation of time intervals in OLT for data transfer to ONT.

A logical unit of the DBA algorithm is Alloc-ID (allocation) with a corresponding T-CONT (traffic counter) on the ONT side. Data transfer parameters (frequency, transmission window) are separately configured for every Alloc-ID (T-CONT) and are referred to as *service level agreement (SLA)*.

In G.984.3 recommendation, several combinations of SLA parameters are described as T-CONT types. There are several T-CONT types:

- T-CONT type 1 is characterized by the fixed bandwidth component only, and is not eligible to share surplus bandwidth. It is suitable for carrying fixed-rate (or variable-rate with relatively low rate bound) traffic which is sensitive to delay and jitter
- T-CONT type 2 is characterized by the guaranteed bandwidth only, and is not eligible to share surplus bandwidth. It is suitable for carrying on-off type traffic with well-defined rate bound which does not have strict delay and jitter requirements.
- T-CONT type 3 is characterized by guaranteed bandwidth and eligibility to participate in non-guaranteed bandwidth sharing. It is suitable for carrying variable-rate bursty traffic which requires average rate guarantee.
- T-CONT type 4 is characterized by eligibility to share the Best-effort bandwidth with neither fixed nor guaranteed bandwidth provisions. It is suitable for carrying variable-rate bursty traffic which does not exhibit delay sensitivity.
- T-CONT type 5 is characterized by fixed and guaranteed bandwidth and eligibility to share the Best-effort. This type is a consolidation of other T-CONT types which can be applied to most general traffic flows.

The terminal allows configuring up to 256 general allocations, 64 allocations for OMCI service traffic and 128 CBR (constant bitrate) type allocations per channel. When one ONT is connected, one allocation will be assigned as a default one. Thus, if 64 ONT are connected, 64 service allocations will be assigned on the channel. 256 general allocations is enough for data processing, but not enough for more than 4 services processing in the own allocation. You need to follow the rule: $A_{max} = 256 / N - 1$, where A_{max} — the maximum quantity of allocations for user data of an ONT, N — the quantity of ONTs on a channel. If the estimated number of ONT services exceeds A_{max} , a combination of several services should be performed in one allocation. More detailed information you can obtain in Chapter 29.2.2.

DBA parameters are configured in the dba profile. These parameters allow specification of any T-CONT type described in G.984.3. First of all, choose a service class which will define the basic DBA algorithm. After that configure status reporting which defines a type of ONT queues status report. The "fixed-bandwidth", "guaranteed-bandwidth", and "besteffort-bandwidth" parameters define the fixed, guaranteed, and best-effort bandwidth correspondingly. Table 23 shows the correspondence between alloc profile configuration and T-CONT types.

Table 23—Alloc Profile Configuration and T-CONT types

	T-CONT type 1	T-CONT type 2	T-CONT type 3	T-CONT type 4	T-CONT type 5
service-class	cbr	voip	type5	type5	type5
status-reporting	-	+	+	+	+
fixed-bandwidth	+	-	-	-	+
guaranteed-bandwidth	-	+	+	-	+
besteffort-bandwidth	-	-	+	+	+

The following rules apply to dba profile assignment:

- When an ONT service is assigned an dba profile, an Alloc-ID is created for the ONT on the OLT side, and a corresponding T-Cont is configured on the ONT side.
- If different ONTs are assigned the same profile, they will each have a separate Alloc-ID created with the same allocation parameters.
- If different services of one ONT are assigned the same alloc profile, the services will operate with one allocation.
- If different services of one ONT are assigned different dba profiles, the services will operate with different allocations. The number of Alloc-IDs created for an ONT equals the number of alloc profiles assigned to it.

29.2 DBA Profiles Assignment

29.2.1 Services in Different T-CONTs

Two Alloc-IDs will be allocated in an OLT for an ONT. Each service will operate in its allocation. There will be two T-CONT on the ONT side corresponding to the allocations.

Step 1. The ONT should have two services in different T-CONTs. Assign two dba profiles by using the **profile dba** command.

```
ma4000# configure terminal
ma4000(config)# profile dba ServiceInternet
ma4000(config-dba) ("ServiceInternet")# exit
ma4000(config)# profile dba ServiceVoIP
ma4000(config-dba) ("ServiceVoIP")# exit
```

Step 2. Assign the profiles to services by using the **service <id> profile dba** command.

```
ma4000(config)(if-ont-0/0/0)# service 0 profile dba ServiceInternet
ma4000(config)(if-ont-0/0/0)# service 1 profile dba ServiceVoIP
```

You will have the following configuration:

```
ma4000(config)(if-ont-0/0/0)# do show interface ont 0/0/0 configuration

...
    Service [0]:
        Profile cross connect:                Service1                ONT
Profile Cross Connect 4
        Profile dba:                          ServiceInternet          ONT
Profile DBA 3
        Custom vlan:                          200
        Custom CoS:                          unused
    Service [1]:
        Profile cross connect:                Service2                ONT
Profile Cross Connect 3
        Profile dba:                          ServiceVoIP              ONT
Profile DBA 4
        Custom vlan:                          200
        Custom CoS:                          unused
...
```

Step 3. Apply the changes by using the **do commit** command.

```
ma4000(config)(if-ont-0/0/0)# do commit
```

29.2.2 Services in One T-CONT

One Alloc-ID will be allocated in an OLT for an ONT. One T-CONT will be configured in the ONT. The T-CONT will be used to transfer traffic from multiple services. Traffic priority will be based on the value of the "priority-queue" field of the corresponding cross-connect profiles.

Step 1. The ONT should have three services in one T-CONT. Assign an dba profile by using the **profile dba** command.

```
ma4000(config)# profile dba AllServices
```

Step 2. Assign the profile to three services by using the **service <id> profile dba** command.

```
ma4000(config)(if-ont-0/0/1)# service 0 profile dba AllServices
ma4000(config)(if-ont-0/0/1)# service 1 profile dba AllServices
ma4000(config)(if-ont-0/0/1)# service 2 profile dba AllService
```

You will have the following configuration:

```
ma4000(config)(if-ont-0/0/1)# do show interface ont 0/0/1 configuration
...
    Service [0]:
        Profile cross connect:          Servicel          ONT
Profile Cross Connect 4
        Profile dba:                    AllServices        ONT
Profile DBA 2
    Service [1]:
        Profile cross connect:          unassigned
        Profile dba:                    AllServices        ONT
Profile DBA 2
    Service [2]:
        Profile cross connect:          unassigned
        Profile dba:                    AllServices        ONT
Profile DBA 2
...
```

Step 3. Apply the changes by using the **do commit** command.

```
ma4000(config)(if-ont-0/0/1)# do commit
```

29.2.3 One Profile for Multiple ONTs

This represents a typical scenario for most cases, when similar services require the same DBA parameters on different ONTs.

Step 1. Assign an dba profile by using the **profile dba** command.

```
ma4000(config)# profile dba ServiceInternet
ma4000(config-dba)("ServiceInternet")#
```

Step 2. Assign the profile to a corresponding service of every ONT by using the **service <id> profile dba** command.

```
ma4000(config)# interface ont 0/0/0-1
ma4000(config)(if-ont-0/0/0-1)# service 0 profile dba ServiceInternet
```

You will have the following ONT configurations:

```
ma4000(config)(if-ont-0/0/0-1)# do show interface ont 0/0/0-1 configuration

-----
[ONT0/0/0] configuration
-----

...
Service [0]:
  Profile cross connect:      Service1      ONT Profile Cross Connect 4
  Profile dba:                ServiceInternet  ONT Profile DBA 3
  Custom vlan:                200
  Custom CoS:                 unused
...
-----
[ONT0/0/1] configuration
-----

...
Service [0]:
  Profile cross connect:      Service1      ONT Profile Cross Connect 4
  Profile dba:                ServiceInternet  ONT Profile DBA 3
...

```

Step 3. Apply the changes by using the **config commit** command.

```
ma4000(config)(if-ont-0/0/0-1)# do commit
```

29.2.4 Profiles Assignment Example

Consider two ONTs which need to have the following three services: Internet, VoIP, and Alarm. The VoIP service should operate in a separate allocation (a definite throughput should be ensured). The Internet and SecurityAlarm services may operate in one allocation.

This configuration implies that an OLT allocates two Alloc-IDs to each ONT. The Internet and SecurityAlarm services operate in one allocation, the VoIP service uses another one. Each ONT has two T-CONT configured which correspond to the Alloc-IDs of the ONT. Traffic priority between the Internet and SecurityAlarm services on the ONT side is based on the "priority-queue" value of the "ServiceInternet" and "ServiceAlarm" cross-connect profiles, which were assigned to the services.

Step 1. Assign two dba profiles by using the **profile dba** command.

```
ma4000(config)# profile dba ServiceVoIP
ma4000(config-dba)("ServiceVoIP")# exit
ma4000(config)# profile dba OtherServices
ma4000(config-dba)("OtherServices")#
```

Step 2. Assign the profiles to corresponding services of every ONT by using the **service <id> profile dba** command.

```
ma4000(config)# interface ont 0/0/0-1
ma4000(config)(if-ont-0/0/0-1)# service 0 profile dba OtherServices
ma4000(config)(if-ont-0/0/0-1)# service 1 profile dba ServiceVoIP
ma4000(config)(if-ont-0/0/0-1)# service 2 profile dba OtherServices
```

You will have the following ONT configurations:

```
ma4000(config)(if-ont-0/0/0-1)# do show interface ont 0/0/0-1 configuration

-----
[ONT0/0/0] configuration
-----

```

```

-----
...
Service [0]:
  Profile cross connect:      Service1      ONT Profile Cross Connect 4
  Profile dba:                ServiceVoIP  ONT Profile DBA 4
  Custom vlan:                200
  Custom CoS:                unused
Service [1]:
  Profile cross connect:      Service2      ONT Profile Cross Connect 3
  Profile dba:                ServiceVoIP  ONT Profile DBA 4
  Custom vlan:                200
  Custom CoS:                unused
Service [2]:
  Profile cross connect:      unassigned
  Profile dba:                OtherServices  ONT Profile DBA 5
...
-----
[ONT0/0/1] configuration
-----
...
Service [0]:
  Profile cross connect:      Service1      ONT Profile Cross Connect 4
  Profile dba:                ServiceVoIP  ONT Profile DBA 4
Service [1]:
  Profile cross connect:      unassigned
  Profile dba:                ServiceVoIP  ONT Profile DBA 4
Service [2]:
  Profile cross connect:      unassigned
  Profile dba:                OtherServices  ONT Profile DBA 5
...

```

Step 3. Apply the changes by using the **commit** command.

```
ma4000(config)(if-ont-0/0/0-1)# do commit
```

29.3 DBA Configuration

29.3.1 T-CONT Type 1 Configuration

Consider configuration of a 100 Mbps fixed bandwidth.

Step 1. Specify a T-CONT type by using the **sla class** command.

```
ma4000(config)# profile dba dba-00
ma4000(config-dba)("dba-00")# sla class cbr
```

Step 2. Specify a type of status reports for ONT queues by using the **sla status-reporting nsr** command.

```
ma4000(config-dba)("dba-00")# sla status-reporting nsr
```

Step 3. Set fixed bandwidth parameters by using the **bandwidth fixed** command. Set other bandwidth parameters to 0.



The bandwidth has a value in Kbps (1000 bps) and is not rounded down to 64 Kbps.

```
ma4000(config-dba)("dba-00")# bandwidth fixed 100000
ma4000(config-dba)("dba-00")# bandwidth guaranteed 0
ma4000(config-dba)("dba-00")# bandwidth besteffort 0
```

Step 4. Use the **show** command to check the parameters.

```
ma4000(config-dba) ("dba-00")# do show profile dba dba-00
Name:                                     'dba-00'
Description:                             'ONT Profile DBA 0'
Dba:
    Sla data:
        Service class:                    cbr
        Status reporting:                 nsr
        Alloc size:                       0
        Alloc period:                     0
        Fixed bandwidth:                  100000
        Guaranteed bandwidth:             0
        Besteffort bandwidth:             0
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-dba) ("dba-00")# do commit
```

29.3.2 T-CONT Type 2 Configuration

Consider configuration of a 100 Mbps guaranteed bandwidth.

Step 1. Specify a T-CONT type by using the **sla class** command.

```
ma4000(config)# profile dba dba-00
ma4000(config-dba) ("dba-00")# sla class voip
```

Step 2. Specify a type of status reports for ONT queues by using the **sla status-reporting** command.

```
ma4000(config-dba) ("dba-00")# sla status-reporting nsr
```

Step 3. Set guaranteed bandwidth parameters by using the **bandwidth guaranteed** command. Set other bandwidth parameters to 0.



The bandwidth has a value in Kbps (1000 bps) and is not rounded down to 64 Kbps.

```
ma4000(config-dba) ("dba-00")# bandwidth fixed 0
ma4000(config-dba) ("dba-00")# bandwidth guaranteed 100000
ma4000(config-dba) ("dba-00")# bandwidth besteffort 0
```

Step 4. Use the **show** command to check the parameters.

```
ma4000(config-dba) ("dba-00")# do show profile dba dba-00
Name:                                     'dba-00'
Description:                             'ONT Profile DBA 0'
Dba:
    Sla data:
        Service class:                    voip
        Status reporting:                 nsr
        Alloc size:                       0
        Alloc period:                     0
        Fixed bandwidth:                  0
        Guaranteed bandwidth:             100000
        Besteffort bandwidth:             0
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-dba) ("dba-00")# do commit
```

29.3.3 T-CONT Type 3 Configuration

Consider configuration of a 100 Mbps guaranteed bandwidth with a possibility of allocation of a 200 Mbps best-effort bandwidth.

Step 1. Specify a T-CONT type by using the **sla class** command.

```
ma4000(config)# profile dba dba-00
ma4000(config-dba) ("dba-00")# sla class type5
```

Step 2. Specify a type of status reports for ONT queues by using the **sla status-reporting** command.

```
ma4000(config-dba) ("dba-00")# sla status-reporting nsr
```

Step 3. Set guaranteed bandwidth parameters by using the **bandwidth guaranteed** command. Set best-effort bandwidth parameters by using the **bandwidth besteffort** command. Set other bandwidth parameters to 0.



The bandwidth has a value in Kbps (1000 bps) and is not rounded down to 64 Kbps.

```
ma4000(config-dba) ("dba-00")# bandwidth fixed 0
ma4000(config-dba) ("dba-00")# bandwidth guaranteed 100000
ma4000(config-dba) ("dba-00")# bandwidth besteffort 200000
```

Step 4. Use the **show** command to check the parameters.

```
ma4000(config-dba) ("dba-00")# do show profile dba dba-00
Name:                                     'dba-00'
Description:                             'ONT Profile DBA 0'
Dba:
    Sla data:
        Service class:                     type5
        Status reporting:                  nsr
        Alloc size:                        0
        Alloc period:                      0
        Fixed bandwidth:                   0
        Guaranteed bandwidth:              100000
        Besteffort bandwidth:              200000
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-dba) ("dba-00")# do commit
```

29.3.4 T-CONT Type 4 Configuration

Consider configuration of a 200 Mbps best-effort bandwidth without allocation of a guaranteed bandwidth.

Step 1. Specify a T-CONT type by using the **sla class** command.

```
ma4000(config)# profile dba dba-00
ma4000(config-dba) ("dba-00")# sla class type5
```

Step 2. Specify a type of status reports for ONT queues by using the **sla status-reporting** command.

```
ma4000(config-dba) ("dba-00")# sla status-reporting nsr
```

Step 3. Set best-effort bandwidth parameters by using the **bandwidth besteffort** command. Set other bandwidth parameters to 0.



The bandwidth has a value in Kbps (1000 bps) and is not rounded down to 64 Kbps.

```
ma4000(config-dba) ("dba-00")# bandwidth fixed 0
ma4000(config-dba) ("dba-00")# bandwidth guaranteed 0
ma4000(config-dba) ("dba-00")# bandwidth besteffort 200000
```

Step 4. Use the **show** command to check the parameters.

```
ma4000(config-dba) ("dba-00")# do show profile dba dba-00\
Name:                                     'dba-00'
Description:                             'ONT Profile DBA 0'
Dba:
  Sla data:
    Service class:                        type5
    Status reporting:                     nsr
    Alloc size:                           0
    Alloc period:                         0
    Fixed bandwidth:                      0
    Guaranteed bandwidth:                 0
    Besteffort bandwidth:                 200000
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-dba) ("dba-00")# do commit
```

29.3.5 T-CONT Type 5 Configuration

Consider configuration of a 100 Mbps fixed bandwidth and a 200 Mbps guaranteed bandwidth with a possibility of allocation of a 1244 Mbps best-effort bandwidth.

Step 1. Specify a T-CONT type by using the **sla class** command.

```
ma4000(config)# profile dba dba-0
ma4000(config-dba) ("dba-00")# sla class type5
```

Step 2. Specify a type of status reports for ONT queues by using the **sla status-reporting** command.

```
ma4000(config-dba) ("dba-00")# sla status-reporting nsr
```

Step 3. Specify fixed bandwidth parameters in the **bandwidth fixed** command, guaranteed bandwidth parameters in the **bandwidth guaranteed** command, and best-effort bandwidth parameters in the **bandwidth besteffort** command.



The bandwidth has a value in Kbps (1000 bps) and is not rounded down to 64 Kbps.

```
ma4000(config-dba)("dba-00"># bandwidth fixed 100000
ma4000(config-dba)("dba-00"># bandwidth guaranteed 200000
ma4000(config-dba)("dba-00"># bandwidth besteffort 1244000
```

Step 4. Use the "show" command to check the parameters.

```
ma4000(config-dba)("dba-00"># do show profile dba dba-00
  Name:                                     'dba-00'
  Description:                             'ONT Profile DBA 0'
  Db:
    Sla data:
      Service class:                       type5
      Status reporting:                    nsr
      Alloc size:                          0
      Alloc period:                        0
      Fixed bandwidth:                     100000
      Guaranteed bandwidth:                200000
      Besteffort bandwidth:                1244000
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-dba)("dba-00"># do commit
```


30 RG ONT CONFIGURATION

30.1 Introduction

This Chapter considers issues related to configuration of Residential Gateway (RG) ONT. The Chapter uses the terms of "bridges" and "routed" services.

Consider the concept of OMCI and RG management domains. These terms are defined in TR-142 Issue 2. In terms of management domains, ONT is considered as a device which operates in an OMCI domain only. The devices which operate in both management domains (i. e. have an integrated router) are denoted ONT/RG. Everything that refers to OMCI domain can be applied to both ONT and ONT/RG devices. For this reason, we will further denote ONT/RG as ONT. If an ONT is configured without an RG domain (without a router), skip all steps concerning RG.

Figure 39 shows ONT/RG scheme and its management domains.

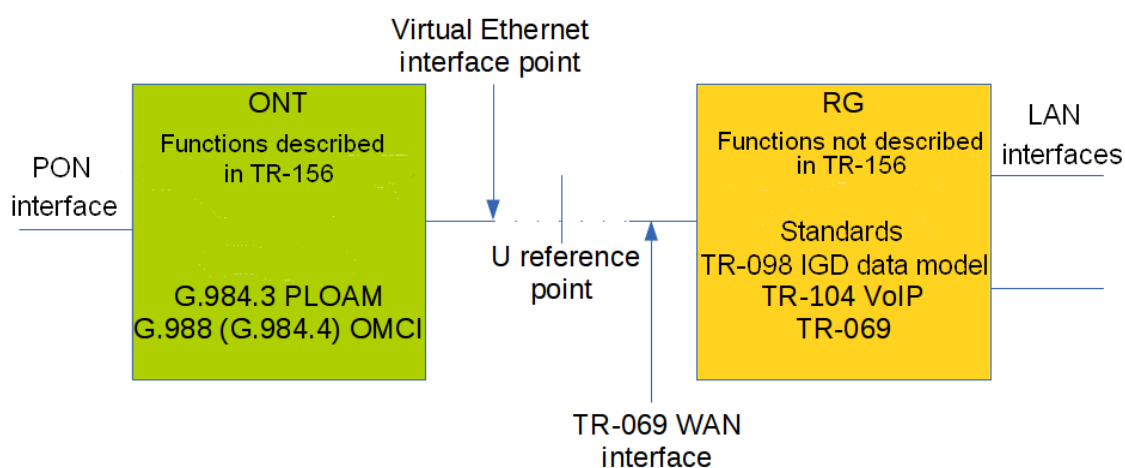


Fig. 39—ONT/RG Management Domains



Bridged service is a service which configuration requires OMCI management domain only, i. e. it can be completely configured with the help of the OMCI protocol in ONT.

Routed service is a service which configuration requires both OMCI and RG management domains.

In addition to configuration in access node, a routed service requires an RG domain to be configured by using one of the following methods:

1. Pre-defined configuration—subscriber is provided with an ONT having fixed configuration.
2. Local ONT configuration using WEB interface.
3. ONT configuration using TR-069 protocol and auto configuration server (ACS).



Contact ONT vendor for information about RG domain configuration.

ONT is connected to RG using a Virtual Ethernet interface point (VEIP), which corresponds to TR-069 WAN interface (described in TR-098) on RG the side. VEIP is represented by a virtual port in access node parameters. The port has the same configuration procedure as Ethernet ports in the "ports" profile.

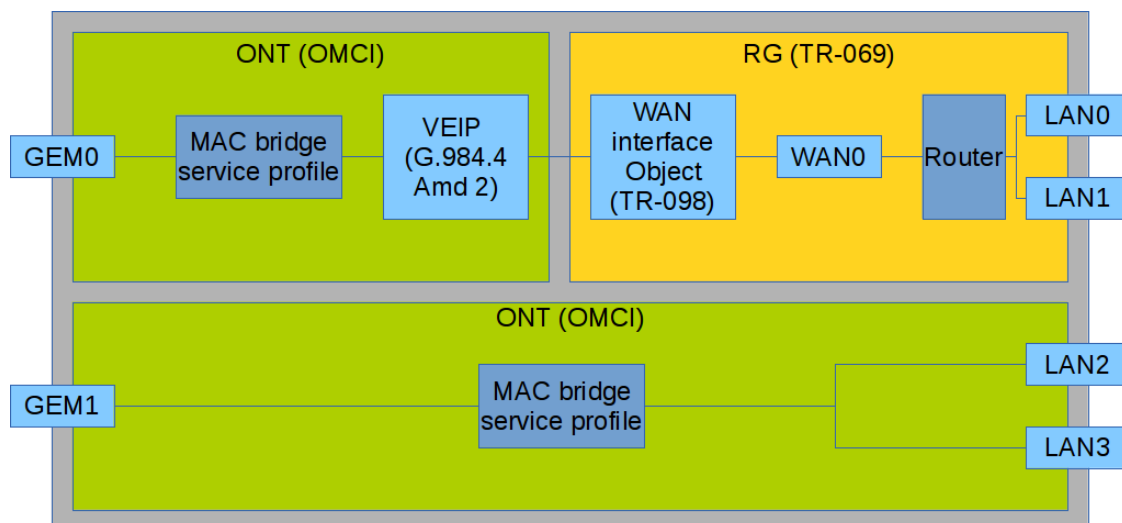


Fig. 40—Services Configuration in ONT and RG Domains

Fig. 40 shows two services (each with a corresponding GEM port on the ONT side), with one of them being **routed** and using both OMCI and RG management domains, and another one being **bridged** and using only OMCI for configuration. Access node configuration includes configuration of bridge interfaces (green areas in the figure) and distribution of LAN ports between management domains.

The **bridge** parameter of the **cross-connect** profile is responsible for association of a service with a management domain. **Bridge** parameter creates a **bridged service** (the **bridge-group** parameter is the bridge number in this case). **No bridge** parameter creates a **routed service** (there is only one bridge associated with the RG; it has a special bridge number—0).

30.2 Services Combined Configuration

Consider an example of ONT configuration which simultaneously uses both management domains. Port numbers and internal structure are shown in Fig. 40.

Step 1. Create a VLAN for services on switch. VLAN configuration is described in details in Chapter [13 VLAN Configuration](#), page [56](#).

```
ma4000(config)# vlan 20
ma4000(vlan-20)# tagged plc-front-port 0/0
ma4000(vlan-20)# tagged plc-pon-port 0/0-1
ma4000(vlan-20)# exit
ma4000(config)# vlan 30
ma4000(vlan-30)# tagged plc-front-port 0/0
ma4000(vlan-30)# tagged plc-pon-port 0/0-1
```

Step 2. Specify "3" service model that corresponds to "VLAN for Service" by using the **gpon olt model** command.

```
ma4000# configure terminal
ma4000(config)# gpon olt model 3
```

Step 3. Create **cross-connect** profiles for services.

```
ma4000(config)# profile cross-connect RG-service
ma4000(config-cross-connect) ("RG-service")# exit
ma4000(config)# profile cross-connect OMCI-service
ma4000(config-cross-connect) ("OMCI-service")#
ma4000(config-cross-connect) ("OMCI-service")# exit
```

Step 4. Create an dba profile. DBA parameters are not important for the purposes set forth in this Chapter, so we will not configure DBA here and simply use default values. We will also assign one profile to both services that means that upstream services will operate with one T-CONT. DBA configuration is described in details in Chapter

```
ma4000(config)# profile dba basic
ma4000(config-dba) ("basic")# exit
```

Step 5. Create a "ports" profile.

```
ma4000(config)# profile ports 2RG-2OMCI
ma4000(config-ports) ("2RG-2OMCI")# exit
```

Step 6. Configure a routed service. Use one VLAN 20 on both the OLT and ONT sides. Set the **routed service** by using the **bridge** command. Configure a cross-connect profile for the routed service.

```
ma4000(config)# profile cross-connect RG-service
ma4000(config-cross-connect) ("RG-service")# no bridge
ma4000(config-cross-connect) ("RG-service")# type general
ma4000(config-cross-connect) ("RG-service")# tag-mode single-tagged
ma4000(config-cross-connect) ("RG-service")# outer vid 20
ma4000(config-cross-connect) ("RG-service")# outer cos unused
ma4000(config-cross-connect) ("RG-service")# user vid untagged
ma4000(config-cross-connect) ("RG-service")# mac-table-limit unlimited
ma4000(config-cross-connect) ("RG-service")# priority 0
```

Step 7. Configure a bridged service. Use one VLAN 30 on both the OLT and ONT sides. Set the **bridged service** by using the **bridge** command. Set the OMCI bridge number to 1. Configure a cross-connect profile for the bridged service.

```
ma4000(config)# profile cross-connect OMCI-service
ma4000(config-cross-connect) ("OMCI-service")# bridge
ma4000(config-cross-connect) ("OMCI-service")# bridge group 1
ma4000(config-cross-connect) ("OMCI-service")# type general
ma4000(config-cross-connect) ("OMCI-service")# tag-mode single-tagged
ma4000(config-cross-connect) ("OMCI-service")# outer vid 30
ma4000(config-cross-connect) ("OMCI-service")# outer cos unused
ma4000(config-cross-connect) ("OMCI-service")# user vid untagged
ma4000(config-cross-connect) ("OMCI-service")# mac-table-limit unlimited
ma4000(config-cross-connect) ("OMCI-service")# priority 1
```

You specified different **priority-queue** values for the services. The routed service will have a higher priority than the **bridged service** as they work with one T-CONT.

Step 8. Configure a **ports** profile. According to Fig. 40, we need to associate the first two LAN ports with an RG management domain, with another two being associated with an OMCI domain and bound to bridge 1.

```
ma4000(config)# profile ports 2RG-2OMCI
ma4000(config-ports) ("2RG-2OMCI")# port 0 bridge group 0
```

```
ma4000(config-ports) ("2RG-2OMCI") # port 1 bridge group 0
ma4000(config-ports) ("2RG-2OMCI") # port 2 bridge group 1
ma4000(config-ports) ("2RG-2OMCI") # port 3 bridge group 1
```

Step 9. Create an ONT configuration. ONT management is described in details in Chapter [28 ONT Configuration](#), page [94](#).

```
ma4000(config) # interface ont 0/0/0
ma4000(config) (if-ont-0/0/0) #
```

Step 10. Assign the created profiles. Assign the **cross-connect RG-service** profile to service 0 and the **cross-connect OMCI-service** profile to service 1.

```
ma4000(config) # interface ont 0/0/0
ma4000(config) (if-ont-0/0/0) # serial ELTX10203040
ma4000(config) (if-ont-0/0/0) # service 0 profile cross-connect RG-service
ma4000(config) (if-ont-0/0/0) # service 0 profile dba basic
ma4000(config) (if-ont-0/0/0) # service 1 profile cross-connect OMCI-service
ma4000(config) (if-ont-0/0/0) # service 1 profile dba basic
ma4000(config) (if-ont-0/0/0) # profile ports 2RG-2OMCI
```

Step 11. Use the **show interface ont <id> configuration** command to check the created configuration.

```
ma4000(config) (if-ont-0/0/0) # do show interface ont 0/0/0 configuration

-----
[ONT0/0/0] configuration
-----

Description:                               ''
Status:                                       UP
Serial:                                     ELTX10203040
...

Service [0]:
  Profile cross connect:                    RG-service      ONT Profile Cross
Connect 6
  Profile dba:                             basic            ONT Profile DBA 6
  Custom vlan:                             200
  Custom CoS:                              unused
Service [1]:
  Profile cross connect:                    OMCI-service    ONT Profile Cross
Connect 7
  Profile dba:                             basic            ONT Profile DBA 6
  Custom vlan:                             200
  Custom CoS:                              unused
...
Profile shaping:                           shaping-00         ONT Profile Shaping 0
Profile ports:                             2RG-2OMCI        ONT Profile Ports 2
Profile management:                        management-00    ONT Profile Management 0
Profile scripting:                         unassigned
Custom model:                             none
Template:                                 unassigned
```

Step 12. Apply the changes by using the **do commit** command.

```
ma4000(config) (if-ont-0/0/0) # do commit
```

As a result, you will have the ONT combined configuration. One of the services is completely managed by the OMCI domain (the bridged service), LAN2 and LAN3 ports are connected as bridges in ONT. The second service is managed by both OMCI and RG (the routed service; RG domain can be configured, for instance, through WEB interface in ONT). LAN0 and LAN1 ports are connected to RG ONT.

31 HIGH SPEED INTERNET CONFIGURATION

Configuration of the High Speed Internet (HSI) service does not have any peculiarities and can be easily performed as described in Chapter 28 ONT Configuration, page 94.

32 MULTICAST CONFIGURATION

32.1 Introduction

The Chapter describes peculiarities of multicast service configuration for model 1 and model 3.

32.2 Model 1 Multicast Configuration

Let us configure a multicast service for model 1.

An STB, which works in VLAN 14, is connected to an ONT port in this example. Upstream IGMP packets arrive at VLAN 14 through a GEM port and the OLT changes VLAN 14 to subscriber's VLAN 200.

As we have a multicast server in VLAN 98 in our example, we need to configure a proxy in switch to translate IGMP packets from VLAN 200 to VLAN 98 (see [13 VLAN Configuration](#), page 56). The multicast service comes downstream to the ONT port in VLAN 98 and changes to VLAN 14.

For more details on general configuration principles of data communication channel refer to Chapter [28 ONT Configuration](#), page 94.

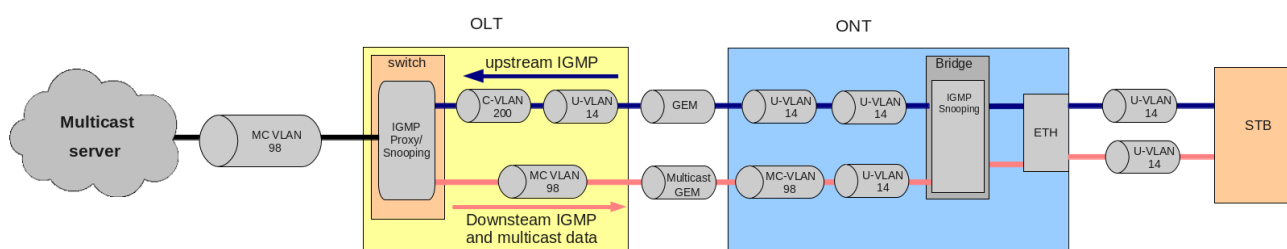


Fig. 41—Model 1 Multicast

Step 1. Specify ONT serial number in configuration.

```
ma4000# configure terminal
ma4000(config)# interface ont 0/0/0
ma4000(config-if-ont-0/0/0)# serial ELTX01234567
ma4000(config-if-ont-0/0/0)# exit
```

Step 2. Assign a service model:

```
ma4000(config)# gpon olt model 1
```

Step 3. Create a "UsIGMP" cross-connect profile to configure the service which will be used to send IGMP requests upstream. Configure a bridged service and specify the bridged group (it equals 1 in our example) the ONT port will be associated with. Specify U-VLAN 14:

```
ma4000(config)# profile cross-connect UsIGMP
ma4000(config-cross-connect) ("UsIGMP")# bridge
ma4000(config-cross-connect) ("UsIGMP")# bridge group 1
ma4000(config-cross-connect) ("UsIGMP")# user vid 14
ma4000(config-cross-connect) ("UsIGMP")# do show profile cross-connect UsIGMP
```

Name:	'UsIGMP'
Description:	'ONT Profile Cross Connect
8'	
Model:	ont
Bridge group:	1
Tag mode:	single-tagged
Outer vid:	1
Outer cos:	unused
Inner vid:	-
U vid:	14
U cos:	unused
Mac table entry limit:	unlimited
Type:	general
Iphost eid:	0
Priority queue:	0

Step 4. Associate a bridge port with an ONT port. To do this, create a "ports" profile and assign value 1 to the "bridge group" parameter for the LAN1 port:

```
ma4000(config)# profile ports Ports1
ma4000(config-ports) ("Ports1")# port 1 bridge group 1
```

Step 5. Enable multicast and configure VLAN replacement rules for ONT:

```
ma4000(config-ports) ("Ports1")# port 1 multicast
ma4000(config-ports) ("Ports1")# port 1 igmp downstream vid 14
ma4000(config-ports) ("Ports1")# port 1 igmp downstream tag-control replace-vid
ma4000(config-ports) ("Ports1")# port 1 igmp upstream vid 14
ma4000(config-ports) ("Ports1")# port 1 igmp upstream tag-control replace-vid
```

Step 6. You also need to configure VLAN 98 multicast and specify the group range:

```
ma4000(config-ports) ("Ports1")# igmp multicast dynamic-entry 0 vid 98
ma4000(config-ports) ("Ports1")# igmp multicast dynamic-entry 0 group 224.0.0.0
239.255.255.255
ma4000(config-ports) ("Ports1")# do show profile ports Ports1
Name:                               'Ports1'
Description:                         'ONT Profile Ports 1'
Igmp settings:
  Version:                           3
  Mode:                               snooping
  Immediate leave:                   false
  Robustness:                         2
  Querier ip:                        0.0.0.0
  Query interval:                     125
  Query response interval:            100
  Last member query interval:         10
  Multicast dynamic entry [0]:
    Vlan id:                          98
    First group ip:                    224.0.0.0
    Last group ip:                     239.255.255.255
...
Port [1]:
  Bridge group:                       1
  Spanning tree for bridge group:     false
  Multicast enable:                   true
  Multicast port settings:
    Upstream igmp vid:                 14
    Upstream igmp prio:                 0
    Upstream igmp tag control:          replace vid
    Downstream multicast vid:           14
    Downstream multicast prio:           0
    Downstream multicast tag control:    replace vid
    Max groups:                         0
    Max multicast bandwidth:            0
```

Shaper downstream:	
Enable:	false
Committed rate:	1000000
Shaper upstream:	
Enable:	false
Committed rate:	1000000
Committed rate:	1000000

Step 7. Assign the created profiles in ONT. Configure a custom-cross-connect profile, specify C-VLAN 200 and apply the configuration:

```
ma4000(config)# interface ont 0/0/0
ma4000(config)(if-ont-0/0/0)# service 0 profile cross-connect UsIGMP
ma4000(config)(if-ont-0/0/0)# profile ports Ports1
ma4000(config)(if-ont-0/0/0)# service 0 custom cvid 200
ma4000(config)(if-ont-0/0/0)# do commit
```

Step 8. Add VLAN 98 and VLAN 200. Enable IGMP snooping.

```
ma4000# configure terminal
ma4000(config)# vlan 200
ma4000(vlan-200)# tagged plc-front-port 0/0
ma4000(vlan-200)# tagged plc-pon-port 0/0-7
ma4000(vlan-200)# ip igmp snooping enable
ma4000(vlan-200)# exit
ma4000(config)# vlan 98
ma4000(vlan-98)# tagged plc-front-port 0/0
ma4000(vlan-98)# tagged plc-pon-port 0/0-7
ma4000(vlan-98)# ip igmp snooping enable
ma4000(vlan-98)# exit
```

Step 9. Configure IGMP proxy for IGMP packets transmission from VLAN 200 to VLAN 98. Apply the configuration.

```
ma4000(config)# ip igmp proxy report enable
ma4000(config)# ip igmp proxy report range 224.0.0.0 239.255.255.255 from 200 to 98
ma4000(config)# ip igmp snooping enable
ma4000(config)# do commit
```


32.3 Model 2 (3) Multicast Configuration

Let us configure a multicast service for model 3. The multicast service operates in VLAN 98 in our example, an STB operating in VLAN 14 is connected to an ONT port. Upstream IGMP packets come to VLAN 14 in the ONT where VLAN 14 is replaced with VLAN 98, and then the data is further transferred upstream through the GEM port. The multicast service comes downstream to the ONT port in VLAN 98 and changes to VLAN 14. For more details on general configuration principles of data communication channel refer to Chapter [28 ONT Configuration](#), page [94](#).

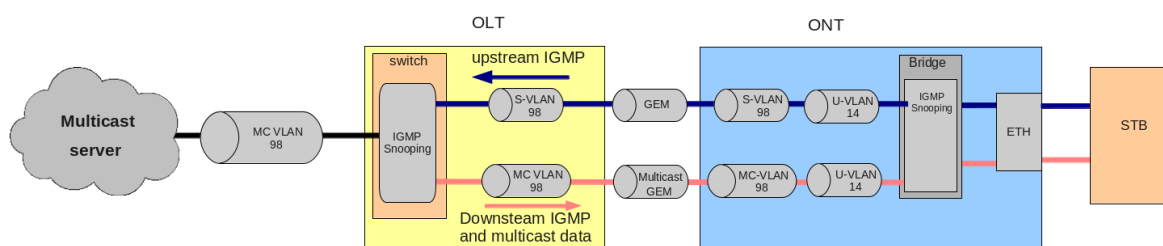


Fig. 42—Model 3 Multicast

Step 1. Add an ONT to the configuration.

```
ma4000# configure terminal
ma4000(config)# interface ont 0/0/0
ma4000(config)(if-ont-0/0/0)# serial ELTX01234567
ma4000(config)(if-ont-0/0/0)# exit
```

Step 2. Assign a service model.

```
ma4000(config)# gpon olt model 3
```

Step 3. Create a "UsIGMP" cross-connect profile to transfer upstream IGMP requests. Configure a bridged service and specify the bridged group (it equals 1 in our example) the ONT port will be associated with. Specify U-VLAN 14 and S-VLAN 98:

```
ma4000(config)# profile cross-connect UsIGMP
ma4000(config-cross-connect) ("UsIGMP")# bridge
ma4000(config-cross-connect) ("UsIGMP")# bridge group 1
ma4000(config-cross-connect) ("UsIGMP")# outer vid 98
ma4000(config-cross-connect) ("UsIGMP")# user vid 14
ma4000(config-cross-connect) ("UsIGMP")# do show profile cross-connect UsIGMP
Name: 'UsIGMP'
Description: 'ONT Profile Cross Connect
8'
Model: ont
Bridge group: 1
Tag mode: single-tagged
Outer vid: 98
Outer cos: unused
Inner vid: -
U vid: 14
U cos: unused
Mac table entry limit: unlimited
Type: general
Iphost eid: 0
Priority queue: 0
```

Step 4. Associate a bridge port with an ONT port. To do this, create a "ports" profile and assign value 1 to the "bridge group" parameter for the LAN1 port:

```
ma4000(config)# profile ports Ports1
ma4000(config-ports) ("Ports1")# port 1 bridge group 1
```

Step 5. Enable multicast and configure VLAN replacement rules for the ONT port (upstream and downstream):

```
ma4000(config-ports) ("Ports1")# port 1 multicast
ma4000(config-ports) ("Ports1")# port 1 igmp downstream vid 14
ma4000(config-ports) ("Ports1")# port 1 igmp downstream tag-control replace-vid
ma4000(config-ports) ("Ports1")# port 1 igmp upstream vid 98
ma4000(config-ports) ("Ports1")# port 1 igmp upstream tag-control replace-vid
```

Step 6. You also need to configure VLAN 98 multicast and specify the group range:

```
ma4000(config-ports) ("Ports1")# igmp multicast dynamic-entry 0 vid 98
ma4000(config-ports) ("Ports1")# igmp multicast dynamic-entry 0 group 224.0.0.0
239.255.255.255
ma4000(config-ports) ("Ports1")# do show profile ports Ports1
  Name:                               'Ports1'
  Description:                         'ONT Profile Ports 1'
  Igmp settings:
    Version:                           3
    Mode:                              snooping
    Immediate leave:                   false
    Robustness:                         2
    Querier ip:                        0.0.0.0
    Query interval:                     125
    Query response interval:            100
    Last member query interval:         10
    Multicast dynamic entry [0]:
      Vlan id:                          98
      First group ip:                   224.0.0.0
      Last group ip:                    239.255.255.255
  ...
  Port [1]:
    Bridge group:                       1
    Spanning tree for bridge group:     false
    Multicast enable:                   true
    Multicast port settings:
      Upstream igmp vid:                 98
      Upstream igmp prio:                0
      Upstream igmp tag control:         replace vid
      Downstream multicast vid:          14
      Downstream multicast prio:         0
      Downstream multicast tag control:  replace vid
      Max groups:                        0
      Max multicast bandwidth:           0
    Shaper downstream:
      Enable:                           false
      Committed rate:                   1000000
    Shaper upstream:
      Enable:                           false
      Committed rate:                   1000000
```

Step 7. Assign the created profiles in ONT and apply the configuration.

```
ma4000(config)# interface ont 0/0/0
ma4000(config) (if-ont-0/0/0)# service 0 profile cross-connect UsIGMP
ma4000(config) (if-ont-0/0/0)# profile ports Ports1
ma4000(config) (if-ont-0/0/0)# do commit
```

Step 8. Add VLAN 98 and enable IGMP snooping:

```
ma4000(config)# vlan 98
ma4000(vlan-98)# tagged plc-front-port 0/0
ma4000(vlan-98)# tagged plc-pon-port 0/0-7
ma4000(vlan-98)# ip igmp snooping enable
ma4000(vlan-98)# exit
ma4000(config)# ip igmp snooping enable
ma4000(config)# do commit
```

33 VOIP CONFIGURATION

33.1 Introduction

The Chapter describes peculiarities of VoIP service configuration.

The access node supports several methods of VoIP configuration:

- VoIP configuration in OMCI management domain;
- VoIP configuration in RG management domain.

A method is chosen based on service model and ONT functionality.

33.2 VoIP Configuration in OMCI Management Domain

VoIP is a special bridged service. It has all general properties of a bridged service. Operator's actions required for services configuration are described in details in Chapter [28 ONT Configuration](#), page [94](#).

As opposed to other bridge services, VoIP has the **iphost** type in the **cross-connect** profile to terminate traffic in internal virtual IP interface. That also requires the **iphost eid** parameter to be specified. As a rule, it should equal 1. Contact your ONT vendor for information about the "iphost eid" value VoIP should have.

Step 1. Configure a cross-connect profile to be used as VoIP.

```
ma4000(config)# profile cross-connect VoIP
ma4000(config-cross-connect) ("VoIP")# bridge
ma4000(config-cross-connect) ("VoIP")# type iphost
ma4000(config-cross-connect) ("VoIP")# bridge group 2
ma4000(config-cross-connect) ("VoIP")# iphost eid 1
```

Step 2. Check the changes made.

```
ma4000(config-cross-connect) ("VoIP")# do show profile cross-connect VoIP
  Name:                               'VoIP'
  Description:                         'ONT Profile Cross Connect
9'
  Model:                              ont
  Bridge group:                       2
  Tag mode:                           single-tagged
  Outer vid:                          1
  Outer cos:                          unused
  Inner vid:                          -
  U vid:                              untagged
  U cos:                              unused
  Mac table entry limit:              unlimited
  Type:                               iphost
  Iphost eid:                         1
  Priority queue:                     0
```

Step 3. Apply the changes by using the **config commit** command.

```
ma4000(config-cross-connect) ("VoIP")# do commit
```

33.3 VoIP Configuration in RG Management Domain

In case a VoIP client is located after the U point (i. e. in an RG management domain), a VoIP service has the same configuration procedure as all other routed services. The procedure is described in details in Chapter [28 ONT Configuration](#), page [94](#). All general steps of service configuration apply to VoIP.

34 TR-069 PROTOCOL MANAGEMENT CONFIGURATION

34.1 Introduction

This Chapter describes configuration of data communication channel for a CPE management service via the TR-069 protocol.

Two modes are available to establish an ONT management channel: Inband and OutOfBand. Inband is a preferred mode as it is simpler. Contact your ONT vendor for information about operation capabilities of both modes.

ONT TR-069 management is a special service. All general steps of service configuration apply to TR-069 management. Operator's actions required for services configuration are described in details in Chapter [28 ONT Configuration](#), page [94](#).

As opposed to other services, a management service has the "management" type specified in the "cross-connect" profile. You also need to specify the "lphost eid" parameter. As a rule, it should equal 0.

34.2 Configuration of a TR-069 Inband management channel

This mode is characterised by its simple implementation. Management traffic goes through the same bridge as user traffic. Fig. 43 shows a part of OMCI scheme. Arrows show the traffic flow.

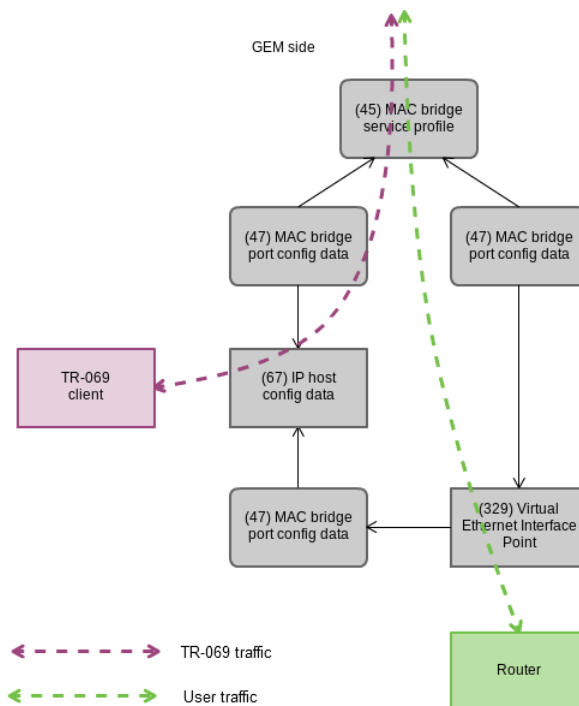


Fig. 43—TR-069 Inband Management Channel

Step 1. Set the "management" type in the "cross-connect" profile.

```
ma4000(config)# profile cross-connect TR069
ma4000(config-cross-connect) ("TR069") # type management
ma4000(config-cross-connect) ("TR069") # no bridge
```

Step 2. Set the "IP Host" identifier to 0.

```
ma4000(config-cross-connect) ("TR069") # iphost eid 0
```

Step 3. Check the changes.

```
ma4000(config-cross-connect) ("TR069") # do show profile cross-connect TR069
Name:                                     'TR069'
Description:                             'ONT Profile Cross Connect
10'
Model:                                    ont-rg
Bridge group:                             -
Tag mode:                                 single-tagged
Outer vid:                                1
Outer cos:                                unused
Inner vid:                                -
U vid:                                    untagged
U cos:                                    unused
Mac table entry limit:                    unlimited
Type:                                     management
Iphost eid:                               0
Priority queue:                           0
```

Step 4. Apply the changes by using the **do commit** command.

```
ma4000(config-cross-connect) ("TR069") # do commit
```

34.3 Configuration of a TR-069 OOB Management Channel

Not all ONT vendors support TR-069 Inband management channel. An OutOfBand alternative management channel is developed for this case. The main peculiarity of the mode is that it uses a separate bridge for management. Provided below is a part of the OMCI scheme. Arrows show the traffic flow.

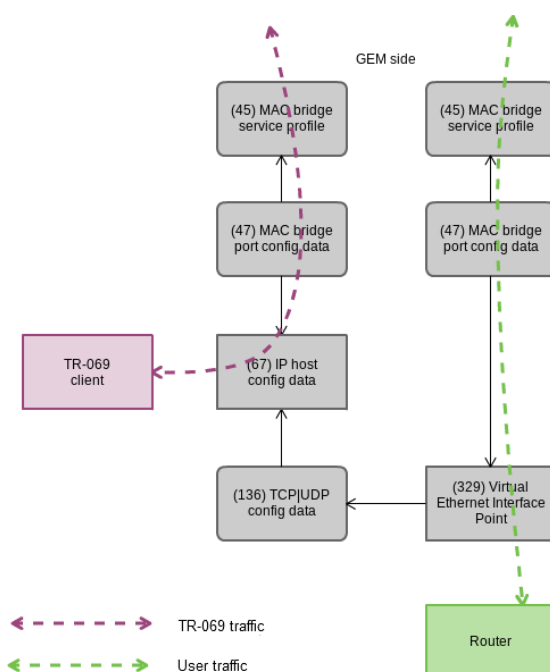


Fig. 44—TR-069 OutOfBand Management Channel

Step 1. Set the "management" type in the "cross-connect" profile.

```
ma4000(config)# profile cross-connect TR069
ma4000(config-cross-connect) ("TR069") # type management
```

Step 2. Set the "ont" model of the "cross-connect" profile. Specify a separate bridge-group.

```
ma4000(config-cross-connect) ("TR069") # bridge
ma4000(config-cross-connect) ("TR069") # bridge group 20
```

Step 3. Set the "IP Host" identifier to 0.

```
ma4000(config-cross-connect) ("TR069") # iphost eid 0
```

Step 4. Check the changes by using the **do show** command.

```
ma4000(config-cross-connect) ("TR069") # do show profile cross-connect TR069
  Name:                                     'TR069'
  Description:                             'ONT Profile Cross Connect
10'
  Model:                                   ont
  Bridge group:                             20
  Tag mode:                                 single-tagged
  Outer vid:                                1
  Outer cos:                                unused
  Inner vid:                                -
  U vid:                                    untagged
  U cos:                                    unused
  Mac table entry limit:                    unlimited
  Type:                                     management
  Iphost eid:                               0
  Priority queue:                           0
```

Step 5. Apply the changes by using the **do commit** command.

```
ma4000(config-cross-connect) ("TR069") # do commit
```

34.4 TR-069 Client Configuration

The **management** profile is used for TR-069 client configuration.

```
ma4000# show profile management management-00
  Name:                                     'management-00'
  Description:                             'ONT Profile Management 0'
  Enable omci configuration:                true
  Url:                                     ''
  Username:                                ''
  Password:                                ''
```

If DHCP server transfers TR-069 parameters using option 43, there is no need in sending the parameters to OMCI. Set the Disable this phrase by using no omci-configuration command.

Otherwise, parameters of the TR-069 client require explicit specification.

Step 1. Enable TR-069 configuration.


```
ma4000# configure terminal
ma4000(config)# profile management management-00
ma4000(config-management) ("management-00")# omci-configuration
```

Step 2. Specify connection parameters.

```
ma4000(config-management) ("management-00")# url http://acs/tele/com:9595/acs
ma4000(config-management) ("management-00")# username acs
ma4000(config-management) ("management-00")# password acsacs
```

Step 3. Check the changes.

```
ma4000(config-management) ("management-00")# do show profile management
management-00
  Name:                               'management-00'
  Description:                         'ONT Profile Management 0'
  Enable omci configuration:           true
  Url:                                'http://acs/tele/com:9595/acs'
  Username:                           'acs'
  Password:                           'acsacs'
```

Step 4. Apply the changes by using the **do commit** command.

```
ma4000(config-management) ("management-00")# do commit
```

35 ONT CONFIGURATIONS TEMPLATES

35.1 Introduction

It is not always convenient, especially for large scale operators, to build ONT configuration from separate profiles for each subscriber. This process is painstaking and risky in a certain sense as it is highly prone to operator error.

As a rule, such companies employ at least one service plan with pre-defined ONT profiles. This Chapter describes ONT templates—an effective solution to simplify the work of subscriber service center specialists.

The essence of configuration templates is simple. Network administrator prepares required quantity of templates for the quantity of service plans. Configuration template contains detailed profile list and a set of ONT parameters. Subscriber service center specialist or OSS/BSS system assigns the template to ONT and identifies additional configuration parameters, if necessary. As a rule, configuration assignment is performed in one click or by using one command.

35.2 ONT Configuration Templates

Step 1. Define ONT Configuration Template.

```
ma4000(config)# template HSI-100-CaTV
ma4000(ont-template) ("HSI-100-CaTV") #
```

Step 2. Set an ONT configuration. Template configuration process does not have any peculiarities and exactly follows ONT configuration process described in Chapter [28 ONT Configuration](#), page [94](#).

```
ma4000(ont-template) ("HSI-100-CaTV") # service 0 profile dba AllServices
ma4000(ont-template) ("HSI-100-CaTV") # service 0 profile cross-connect Service1
ma4000(ont-template) ("HSI-100-CaTV") # service 1 profile dba AllServices
ma4000(ont-template) ("HSI-100-CaTV") # service 1 profile cross-connect Service2
ma4000(ont-template) ("HSI-100-CaTV") # profile ports Ports1
...
```

Step 3. Disable all configuration parameters that should be specified explicitly for ONT with the `undefine` command, if necessary.

```
ma4000(ont-template) ("HSI-100-CaTV") # undefine rf-port-state
...
```

Step 4. Apply the changes made

```
ma4000(ont-template) ("HSI-100-CaTV") # do commit
```

35.3 ONT Configuration Templates Assignment

Step 1. Switch to the ONT view. For group operations, you can use the range of ONT IDs, if necessary.

```
ma4000(config)# interface ont 0/0/0-10
ma4000(config)(if-ont-0/0/0-10)#
```

Step 2. Assign configuration template to ONT by using the template command.

```
ma4000(config)(if-ont-0/0/0-10)# template HSI-100-CaTV
```

Step 3. Define individual ONT parameters not specified in the template, if necessary.

```
ma4000(config)(if-ont-0/0/0-10)# rf-port-state enabled
```

Step 4. Apply the changes made

```
ma4000(config)(if-ont-0/0/0-10)# do commit
```

35.4 ONT Configuration Preview with Templates

ONT configuration viewing is performed by using the **show interface ont <id> configuration** command. [T] markers (Template) allow to discriminate template configuration parameters from the general ones. In this example, **Rf port state** is the only general parameter

```
ma4000(config)(if-ont-0/0/0-10)# do show interface ont 0/0/0 configuration
```

```
-----
[ONT0/0/0] configuration
-----
```

```

Description:                                ''
Enabled:                                     true
Serial:                                     ELTX01234567
Password:                                   '00000000000'
[T] Fec up:                                false
[T] Downstream broadcast:                  true
[T] Ber interval:                          100000
[T] Ber update period:                     60
Rf port state:                             enabled
[T] Omci error tolerant:                   false
Service [0]:
[T]   Profile cross connect:                Service1      ONT Profile Cross Connect 4
[T]   Profile dba:                         AllServices   ONT Profile DBA 2
      Custom vlan:                          200
      Custom CoS:                          unused
Service [1]:
[T]   Profile cross connect:                Service2      ONT Profile Cross Connect 3
[T]   Profile dba:                         AllServices   ONT Profile DBA 2
      Custom vlan:                          200
      Custom CoS:                          unused
Service [2]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
Service [3]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
Service [4]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
Service [5]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
Service [6]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
Service [7]:
[T]   Profile cross connect:                unassigned
[T]   Profile dba:                         unassigned
[T] Profile shaping:                       shaping-00      ONT Profile Shaping 0
[T] Profile ports:                         Ports1         ONT Profile Ports 1
[T] Profile management:                    management-00  ONT Profile Management 0
[T] Profile scripting:                     unassigned
Custom model:                             none
Template:                                 HSI-100-CaTV      ONT Template 1

```

36 ONT LICENSING

36.1 Introduction

By default, the operation with OLT is enabled only for ONT made by Eltex. For other ONTs, you need to activate a license. Please, contact a commercial department of Eltex to obtain a license.



If a third-party ONT is connected to OLT without a license, the following entry will be made in the log file:

2017-01-18 05:11:39 pmchal: error: [ONT2/0] License is not valid, configuration will not continue

36.2 Loading a License File to OLT

The license is a text file of the following format:

```
{
  "version":    "<VER>",
  "type":      "all",
  "count":     "<count>",
  "sn":        "<SN>",
  "mac":       "<MAC>",
  "sign":      "<hash>"
}
```

where:

- *VER* – the version number of a license;
- *count* – the quantity of third-party ONTs that can run on OLT;
- *SN* – a serial number of LTP;
- *MAC* – MAC address of LTP;
- *hash* – digital signature of the license file.

There are two ways to load a license to OLT:

1. Using a 'copy' command:

```
ma4000# copy tftp://<IP>/<PATH> fs://license
Download file from TFTP-server..
License successfully installed. Please reboot device for changes to make effect
```

where:

IP – IP address of TFTP server;

PATH – path to the license file on the TFTP server.

2. Using CLI:

```
ma4000# license set ""<license>""
License successfully installed. Please reboot device for changes to make effect
```

where:

license – the full content of the license file, including curly braces.

For viewing the information on uploaded license, use '**show**' command:

```
ma4000# show license
Active license information:
  License valid:          yes
  Version:               1.1
  Carrier:               Eltex Enterprise LLC
  Licensed vendor:       all
  Licensed ONT count:     unlimited
  Licensed ONT online:    2
  SN:                   OL02000000
  Mac:                   A8:F9:4B:00:00:00
```

The license file is saved while restarting, firmware updating and configuration uploading. The license will remove after resetting of OLT to default settings.

PART V

ACCESS NODE MONITORING

37 GENERAL INFORMATION

37.1 View Current SW Version of Access Node

To view information on the current SW version, **show firmware** command shall be used.

```
ma4000# show firmware

Firmware status:
~~~~~
Unit   Image   Running   Boot           Version          Date
----   -
1      0        No        *              1 3 2 335 40605  23-Oct-2014 09:06:46
1      1        Yes       *              1 3 2 340 40625  24-Oct-2014 20:06:55
2      0        Yes       *              1 3 2 340 40625  24-Oct-2014 20:06:55
2      1        No        *              1 3 2 335 40605  23-Oct-2014 09:06:46

"*" designates that the image was selected for the next boot
```

37.2 View Information on Access Node

To view information on PP4X modules, **show system information** command shall be used. PP4X module number shall be specified as a parameter.

```
ma4000# show system information 1
System information (1):
Uptime (d:h:m:s): 5:22:26:57
CPU load (1/5/15 minutes): 0.00/0.01/0.00
RAM (total/free), Mbytes: 498/287
Partition '/' (total/free), Mbytes: 57/23
Partition '/mnt/tools' (total/free), Mbytes: 1024/934
Partition '/mnt/config' (total/free), Mbytes: 64/61
Partition '/mnt/log' (total/free), Mbytes: 128/123
Temperature (SFP): 35C
Temperature (CPU): 42C
Temperature (Switch) : 49C
Firmware version: 3.22.0.189 r39940 05:32:45 04/09/2014
Linux version: Linux version 2.6.22.18 (alexey.vlasov@turbo.eltex.loc) (gcc
version 4.3.2 (sdk3.2rc1-ct-ng-1.4.1) ) #1 Thu Sep 4 12:02:21 NOVT 2014
MAC address: a8:f9:4b:88:33:a0
Serialnumber: OL02000580
```

To view information about the crate, **show system environment** command shall be used.

```
ma4000# show system environment
MFC board status:      ok
MFC board version:     0x2
MFC firmware:
  Status:              0x00 (ok)
  Version:             8 2 1 1 5 05/11/2013
  Timestamp (UTC):     05-Nov-2013 12:19:22

Fan configured speed, %: auto
Fan current speed, %:  46
Fan minimum speed, %:  15
Fan speed levels, %:   15 25 36 46 57 68 78 89 100

Status:               Fan0      Fan1      Fan2
                    ok        ok        ok
```

RPM:	1524	1554	1560
	Feeder1	Feeder2	
Status:	REVERSED	ok	
Current, A:	0.00	1.00	
Voltage, V:	1.92	-53.69	
Shelfvoltage, V:	-54.35		

37.3 Interface Module Status View

To view information about interface modules, **show shelf** command shall be used.

```
ma4000# show shelf
```

Shelf status ~~~~~						
Slot #	Configured Type	Detected Type	Version	Serial #	Link State	Slot State
0	plc8	plc8	3.22.0.189	OL04001750	up	Operational
1	none	none	0.0.0.0		down	Absent
2	none	none	0.0.0.0		down	Absent
3	none	none	0.0.0.0		down	Absent
4	none	none	0.0.0.0		down	Absent
5	none	none	0.0.0.0		down	Absent
6	none	none	0.0.0.0		down	Absent
7	none	none	0.0.0.0		down	Absent
8	none	none	0.0.0.0		down	Absent
9	none	none	0.0.0.0		down	Absent
10	none	none	0.0.0.0		down	Absent
11	none	none	0.0.0.0		down	Absent
12	none	none	0.0.0.0		down	Absent
13	none	none	0.0.0.0		down	Absent
14	none	none	0.0.0.0		down	Absent
15	none	none	0.0.0.0		down	Absent

37.4 Access Node Uptime View

To view access node uptime, **show uptime** command shall be used.

```
ma4000# show uptime
up 7 days, 20:11
```

37.5 Network Connection Check

In order to check connection to mains, **ping** command shall be used. Transmit IP address of a node being checked as a parameter.

```
ma4000# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254): 56 data bytes
64 bytes from 192.168.1.254: seq=0 ttl=64 time=0.422 ms
64 bytes from 192.168.1.254: seq=1 ttl=64 time=0.426 ms
64 bytes from 192.168.1.254: seq=2 ttl=64 time=0.360 ms
64 bytes from 192.168.1.254: seq=3 ttl=64 time=0.397 ms
64 bytes from 192.168.1.254: seq=4 ttl=64 time=0.404 ms

--- 192.168.1.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.360/0.401/0.426 ms
```


38 ACCESS NODE RUN-TIME LOG

To view a list of logs, **show log** command shall be used:

```
ma4000# show log

Log files
~~~~~
##      Name                Size in bytes      Date of last modification
-----
1       daemon              450                Thu Sep 11 16:59:14 2014
2       pp                  126432             Thu Sep 11 16:59:46 2014
-----
Totalfiles: 2
```

Table 24—Purpose of run-time logs

Name	Description
daemon	Log messages of MA4000 auxiliary services get saved in the log
pp	Log messages of master PP4X module get saved in the log
pp-other	Log messages of slave PP4X module get saved in the log
slot	Log messages of definite interface module get saved in the log.

To view run-time log, **show log** command shall be used. Transmit log name as a parameter.

```
ma4000# show log pp
2014-09-11 16:58:10 rebootd started
2014-09-11 16:58:10 cli-mgr <main>
2014-09-11 16:58:10 cli-mgr <climgr_initialize>
2014-09-11 16:58:10 cli-mgr <main_loop>
2014-09-11 16:58:10 switch %SWITCH: starting up
2014-09-11 16:58:10 switch %SWITCH: start
2014-09-11 16:58:10 syslog-ng syslog-ng starting up; version='3.2.3'
2014-09-11 16:58:10 switch %STARTUP: init
2014-09-11 16:58:10 switch %STARTUP: Position is left
2014-09-11 16:58:10 switch %STARTUP: ShelfId is 15
2014-09-11 16:58:10 switch %FACTORY: reading factory settings...
2014-09-11 16:58:10 switch %FACTORY: OK
2014-09-11 16:58:10 switch %PARSE-CFG: processing configuration file
"/tmp/boot.conf.1"...
2014-09-11 16:58:10 switch %PARSE-CFG: Operation successful.
2014-09-11 16:58:10 switch %PARSE-CFG: Operation successful.
2014-09-11 16:58:10 switch %PARSE-CFG: Operation successful.
2014-09-11 16:58:10 switch %PARSE-CFG: Operation successful.
2014-09-11 16:58:10 switch %PARSE-CFG: Operation successful.
2014-09-11 16:58:10 switch %PARSE-CFG: parse config: ...done.
2014-09-11 16:58:11 switch Device[0] ID 0xE00D11AB revision B1 or above
...
```

Log messages may be filtrated. Use **show log<journal> grep** command to do that. A string of symbols used for making a search in the log is a command parameter. Only those messages that comprise this string will be displayed on the screen.

```
ma4000# showlogppgreppp4x
2014-09-11 16:58:57 switch %FIRMWARE: by entering 'firmware pp4x confirm unit 1'
command in the CLI.
2014-09-11 16:59:46 switch %FIRMWARE: 'firmware pp4x confirm unit 1' command
entered.
```

39 ACTIVE ALARMS LOG

39.1 Introduction

The system of logging is built on a central application systemdb, which organizes interfaces to events database (DB). All emerging events both from interface boards and PP4X switch itself are sent into systemdb to be saved in the base.

All events are divided into 2 types: one-time and state changing events. One-time events are saved in the base and generate SNMP trap, if necessary. State changing events imply the following: if the state has changed (e.g., Link Flapping has been found on interface) and this state is normalized, then we will get a new event indicating situation improvement. State changing events, if they are alarms, are to be added into a list of active alarms during registration in the base. If situation gets corrected the alarm will be removed from active alarms.

39.2 Alarm Generation and Registration

An event can get into the system of logging by two methods: it can be generated at PP4X itself, or on one of interface boards in MA4000 basket. All codes of events in the basket are entered into a common list for convenience to promptly get SNMP OID code for any event.

39.2.1 Structure of Alarm/Event

- Alarm code – code of alarm MA4000, an integer value which can range from 1000 to 7000. PP4X uses a range from 1,000 to 3,000.
- Time – time of occurrence of alarm of this type. The figure is given in seconds from the beginning of epoch.
- Priority – alarm rate. An integer value from 0 to 3.
- Text – a text field with description that can hold up to 255 symbols. The name of alarm as well as auxiliary parameters are always preserved in Text field.
- Params – array of 4 integers specific for every particular alarm or notification.

The Active field will indicate, whether this particular alarm is currently active. The alarm will be active from the time of arriving of the first alarm of this type until arrival of an event for its normalization. E.g.: the state will always be Active for ALARM_LINK_CHANGED after dropping the port unless ALARM_LINK_CHANGED event arrives indicating that the port has recovered again.

- Time field – time of occurrence of the event.

39.2.2 Alarm rates

- Critical – Critical, level 0. Basket operation functionality disturbed.
- Major – High, level 1. Basket separate modules affected.
- Minor – Low, level 2. Non-critical comments in separate modules.
- Notify – Notification, level 3. Not considered as alarm, it informs on the event that happened.

39.2.3 Alarms

Alarms from MA4000_ALARM_SLOT family are generated in case of non-standard situations with interface modules in the basket.

All of them feature the following parameters:

- 0 – slot number
- 1 – device type code
- 2 – device version (hw, major, minor)
- 3 – build of device version

Name:	MA4000_ALARM_SLOT_INVALID
Description:	Alarm occurring when board type in a slot does not correspond to basket configuration.
Alarm rate:	Major
Name:	MA4000_ALARM_SLOT_DOWN
Description:	Alarm in case of link (slot-channel) drop towards interface board.
Alarm rate:	Critical
Name:	MA4000_ALARM_SLOT_ERROR
Description:	Alarm in case of error in connection with interface board. May be caused due to board pending.
Alarm rate:	Critical
Name:	MA4000_ALARM_PP4X_UNIT_LOST
Description:	Alarm on unplanned loss of one of PP4X units in a basket.
Alarm rate:	Critical
Parameters:	0 – number of a missing unit; 1 – RH or LH unit is lost.
Name:	MA4000_ALARM_SYNC_DISALLOWED
Description:	Alarm when configuration synchronization between PP4X units in a basket is disallowed.
Alarm rate:	Critical
Parameters:	0 – number of a unit, with which synchronization is disallowed.
Name:	MA4000_FAN_CONTROLLER_FAIL
Description:	Alarm at controller fans failure.
Alarm rate:	Major
Parameters:	Absent.
Name:	MA4000_CONFIG_SAVE_FAIL
Description:	Alarm at error of PP4X configuration saving to memory.
Alarm rate:	Major
Parameters:	Absent.
Name:	MA4000_ALARM_LINK_DOWN
Description:	Alarm as a result of link drop on PP4X.
Alarm rate:	Minor
Parameters:	0 – idb ID of the interface.
Name:	MA4000_PORT_CNTR_ERRORS_FOUND
Description:	Alarm at revealing errors at PP4X ports.

Alarm rate: Minor
Parameters: 0 – idb ID of port, where errors have been detected.

Name: MA4000_FAN_FAIL
Description: Alarm at failure of either of the basket fans.
Alarm rate: Major
Parameters: 0 – Number of a failing basket fan.

39.2.4 Normalization of Alarms

Name: MA4000_ALARM_SLOT_OK
Description: Notification on interface board being in a normal working condition. It clears all other alarms of MA4000_ALARM_SLOT family for this slot.
Alarm rate: Notify

Name: MA4000_ALARM_PP4X_UNIT_LOST_OK
Description: Notification on revealing PP4X unit lost earlier in the basket.
Alarm rate: Notify
Parameters: 0 – number of a found unit;
1 – RH or LH unit is found.

Name: MA4000_ALARM_SYNC_DISALLOWED_OK
Description: Notification on allowing configuration synchronization with this unit. It clears alarm MA4000_ALARM_SYNC_DISALLOWED.
Alarm rate: Notify
Parameters: 0 – number of a unit, with which synchronization is allowed.

Name: MA4000_FAN_CONTROLLER_FAIL_OK
Description: Notification on restoring serviceability of fans controller. It clears alarm MA4000_FAN_CONTROLLER_FAIL.
Alarm rate: Notify
Parameters: Absent.

Name: MA4000_ALARM_LINK_UP
Description: Notification on a link appearing at port PP4X. It clears alarm MA4000_ALARM_LINK_DOWN for this port.
Alarm rate: Notify
Parameters: 0 – idb ID of the interface.

Name: MA4000_PORT_CNTR_ERRORS_FREE
Description: Notification on discontinued errors at ports PP4X. It clears alarm MA4000_PORT_CNTR_ERRORS_FOUND.
Alarm rate: Notify
Parameters: 0 – idb ID of a port, where no more errors have been detected.

Name: MA4000_FAN_OK
Description: Notification on a fan serviceability restoration. Clears alarm MA4000_FAN_FAIL.
Alarm rate: Notify
Parameters: 0 – number of a fan with restored serviceability.

39.2.5 Reports

Name: MA4000_ALARM_BUFFER_OVERFLOW

Description: A system event occurring in case of alarm queue overflow prior to saving into database.

Alarm rate: Notify

Parameters: 0 – number of alarms lost.

Name: MA4000_ALARM_REBOOT_STACK

Description: Notification on entire basket reboot following a command.

Alarm rate: Notify

Parameters: Absent.

Name: MA4000_ALARM_REBOOT_UNIT

Description: Notification on a separate unit reboot following a command.

Alarm rate: Notify

Parameters:

0 – unit number;

1 – whether this unit was a master.

Name: MA4000_ALARM_REBOOT_FW_TIMER

Description: Notification on expired confirmation timer after firmware update on PP4X board.

Alarm rate: Notify

Parameters: 0 – unit number.

Name: MA4000_ALARM_OMS

Description: Family of notifications on errors at loading/unloading basket configuration through EMS network control system.

Alarm rate: Notify

Parameters:

0 – type of command, which reached completion with an error. Configuration downloading or uploading to a remote server;

1 – field is constant. Indication that the error has occurred during file operation;

2 – code of error, with which operation reached completion.

Name: MA4000_ALARM_OMS_OK

Description: Notification for the EMS network control system on successful downloading/uploading of configuration.

Alarm rate: Notify

Parameters: Absent.

Name: MA4000_ALARM_FW_UPDATE_FAIL

Description: Notification on the error occurred during updating firmware version and libraries for interface boards in MA4000 basket.

Alarm rate: Notify

Parameters: 0 – code of an error, with which operation reached completion.

Name: MA4000_ALARM_FW_UPDATE_OK

Description: Notification on successful updating of firmware version and libraries for interface boards in MA4000 basket.

Alarm rate: Notify

Parameters: Absent.

Name: MA4000_ALARM_FW_CONFIRM_NEEDED

Description: Notification sent to the EMS network control system after updating firmware on PP4X informing on the necessity to perform a *confirm* command.

Alarm rate: Notify

Parameters: 0 – unit number.

Name: MA4000_CONFIG_APPLIED

Description: Notification on PP4X configuration applied.

Alarm rate: Notify

Parameters: 0 – current number of configuration revision

Name: MA4000_CONFIG_SAVED

Description: Notification on PP4X configuration saved to flash memory.

Alarm rate: Notify

Parameters: Absent.

Name: MA4000_CONFIG_RESTORE

Description: Notification on restoration of PP4X configuration or interface board to a previous version. It is a result of a *restore* command; also appears in case of expiry of a timer set for a *confirm* command.

Alarm rate: Notify

Parameters:

0 – type of device, which has rolled back configuration;

1 – slot number (if it is interface board).

Name: MA4000_CSCD_MASTER_CHANGED

Description: Notification on a change of a master in basket.

Alarm rate: Notify

Parameters:

0 – number of a new master unit;

1 – RH or LH unit became a master.

40 PP4X MONITORING

40.1 PP4X Resource Status

To view the command dispatcher information, use the **show cmd-dispatcher** command:

```
ma4000# show cmd-dispatcher
Command Dispatcher memory state:
  overload count      0
  errors              0
  size of element     1192
  free                500
  length              500
```

To view the event dispatcher information, use the **show evt-dispatcher** command:

```
ma4000# show evt-dispatcher
Command Dispatcher memory state:
  overload count      0
  errors              0
  size of element     992
  free                500
  length              500
```

To view the system queue identifiers, use the **show queue** command:

```
ma4000# show queue
Registered queues:
command top manager          id 1
event exchange              id 2
control exchange            id 3
mac sync event descriptors   id 4
mac sync control descriptors id 5
cscd event descriptors       id 6
cscd command descriptors     id 7
config manager event descriptor id 8
config manager command descript id 9
pstate check event descriptors id 10
pstate check control descriptor id 11
sshd event descriptors       id 12
telnetd event descriptors    id 13
firmware manager event descript id 14
firmware manager command descri id 15
maep cmd descriptors         id 16
maep evt descriptors         id 17
vlan cmd descriptors         id 18
vlan evt descriptors         id 19
acsd event descriptors       id 20
fan event descriptors        id 21
arp event descriptors        id 22
arp command descriptors      id 23
iprouting event descriptors   id 24
iprouting command descriptors id 25
igmp snooping event descriptors id 26
igmp snooping command descripto id 27
snmpag evt descriptors       id 28
snmpag cmd descriptors       id 29
bonding event descriptors     id 30
bonding command descriptors   id 31
dhcp client event descriptors id 32
dhcp proxy event descriptors  id 33
dhcp proxy command descriptors id 34
```

```

dhcp server event descriptors      id 35
stp event descriptors             id 36
stp command descriptors           id 37
lldp event descriptors            id 38
lldp command descriptors          id 39
snmp client event descriptors     id 40
Total queues 40

```

To view the state of the selected queue, use the **show queue** command with the queue identifier as a parameter.

```

ma4000# show queue 0
Queue event top manager          :
    tx count                     17
    rx count                     17
    overload count                0
    read from empty count        0
    pipe read errors              0
    pipe write errors             0
    size of element               4
    free                         500
    length                       500

```

40.2 MAC Address Table Preview

To view the MAC address table, use the **show mac pp4** command:

```

ma4000# show mac pp4

Mac table (shadow)
~~~~~
VID      MAC address      Port                      Type      From      To
-----
1        00:80:c2:00:00:00    0/CPU                    Static    Forward   Trap to CPU
1        a8:f9:4b:88:33:a0    1/CPU                    Static    Forward   Trap to CPU
1        00:02:11:22:e3:b8    front-port 1/0           Dynamic   Forward   Forward
1        00:1b:21:4f:f5:ad    front-port 1/0           Dynamic   Forward   Forward
1        00:24:21:a0:9a:80    front-port 1/0           Dynamic   Forward   Forward
1        20:cf:30:bf:ac:61    front-port 1/0           Dynamic   Forward   Forward
1        20:cf:30:e8:0f:28    front-port 1/0           Dynamic   Forward   Forward
1        20:cf:30:e8:0f:66    front-port 1/0           Dynamic   Forward   Forward
1        50:46:5d:8e:27:68    front-port 1/0           Dynamic   Forward   Forward
1        90:e6:ba:1f:c0:41    front-port 1/0           Dynamic   Forward   Forward
1        90:e6:ba:9f:09:99    front-port 1/0           Dynamic   Forward   Forward
1        a8:f9:4b:80:e7:00    front-port 1/0           Dynamic   Forward   Forward
1        a8:f9:4b:80:e7:27    front-port 1/0           Dynamic   Forward   Forward
1        bc:ee:7b:73:dd:af    front-port 1/0           Dynamic   Forward   Forward
1        00:80:c2:00:01:01    slot-channel 0           Static    Forward   Forward
1        a8:f9:4b:88:4f:20    slot-channel 0           Dynamic   Forward   Forward
1        00:80:c2:00:01:02    slot-channel 1           Static    Forward   Forward
1        00:80:c2:00:01:03    slot-channel 2           Static    Forward   Forward
1        00:80:c2:00:01:04    slot-channel 3           Static    Forward   Forward
1        00:80:c2:00:01:05    slot-channel 4           Static    Forward   Forward
1        00:80:c2:00:01:06    slot-channel 5           Static    Forward   Forward
1        00:80:c2:00:01:07    slot-channel 6           Static    Forward   Forward
1        00:80:c2:00:01:08    slot-channel 7           Static    Forward   Forward
1        00:80:c2:00:01:09    slot-channel 8           Static    Forward   Forward
1        00:80:c2:00:01:0a    slot-channel 9           Static    Forward   Forward
1        00:80:c2:00:01:0b    slot-channel 10          Static    Forward   Forward
1        00:80:c2:00:01:0c    slot-channel 11          Static    Forward   Forward
1        00:80:c2:00:01:0d    slot-channel 12          Static    Forward   Forward
1        00:80:c2:00:01:0e    slot-channel 13          Static    Forward   Forward
1        00:80:c2:00:01:0f    slot-channel 14          Static    Forward   Forward
1        00:80:c2:00:01:10    slot-channel 15          Static    Forward   Forward
4094    a8:f9:4b:88:33:a0    1/CPU                    Static    Forward   Trap to CPU
32 valid mac entries

```



```
ma4000# show mac pp4 include vlan 30
```

```
Mac table (shadow)
~~~~~
```

VID	MAC address	Port	Type	From	To
30	a8:f9:4b:82:99:80	port-channel 2	Dynamic	Forward	Forward
30	a8:f9:4b:82:99:93	port-channel 2	Dynamic	Forward	Forward
30	a8:f9:4b:84:e3:40	port-channel 2	Dynamic	Forward	Forward
30	a8:f9:4b:5a:bc:49	slot-channel 2	Dynamic	Forward	Forward

```
4 valid mac entries
```

```
ma4000# show mac slot 2 include vlan 2149
```

```
Mac table (shadow)
~~~~~
```

VID	MAC address	Port	Type	From	To
2149	a8:f9:4b:5a:bc:47	plc-pon-port 2/1 (slot 2)	Dynamic	Unknown	Unknown
2149	00:90:1a:42:be:32	plc-slot-channel 2/0 (slot 2)	Dynamic	Unknown	Unknown

```
2 valid mac entries
ma4000#
```

40.3 PP4X Interface Status Preview

To view the PP4X interface status, use the **show interface <id> status** command:

PP4X interfaces include: front-port, slot-port.

```
ma4000# show interface front-port 1/0-5 status
```

Interface	Status	Media	Speed	Duplex	Flow control
front-port 1/0	up	copper	1 Gbps	full	no
front-port 1/1	down	none	10 Mbps	half	no
front-port 1/2	down	none	10 Mbps	half	no
front-port 1/3	down	none	10 Mbps	half	no
front-port 1/4	down	none	10 Mbps	half	no
front-port 1/5	down	none	10 Mbps	half	no

```
ma4000# show interface slot-channel 0-15 status
```

Interface	Status	Media	Speed	Duplex	Flow control
slot-channel 0	up	none	10 Gbps	full	no
slot-channel 1	down	none	10 Mbps	full	no
slot-channel 2	down	none	10 Mbps	full	no
slot-channel 3	down	none	10 Mbps	full	no
slot-channel 4	down	none	10 Mbps	full	no
slot-channel 5	down	none	10 Mbps	full	no
slot-channel 6	down	none	10 Mbps	full	no
slot-channel 7	down	none	10 Mbps	full	no
slot-channel 8	down	none	10 Mbps	full	no
slot-channel 9	down	none	10 Mbps	full	no
slot-channel 10	down	none	10 Mbps	full	no
slot-channel 11	down	none	10 Mbps	full	no
slot-channel 12	down	none	10 Mbps	full	no
slot-channel 13	down	none	10 Mbps	full	no
slot-channel 14	down	none	10 Mbps	full	no
slot-channel 15	down	none	10 Mbps	full	no

40.4 PP4X Interface Statistics Preview

Step 1. To view the PP4X interface statistics, execute the **show interface <id> counters** command:

PP4X interfaces include: front-port, slot-port.

```
ma4000# show interface front-port 1/0-5 counters
```

Port	UC recv	MC recv	BC recv	Octets recv
-----	-----	-----	-----	-----
--				
front-port 1/0	28880	60669	25654	15133168
front-port 1/1	0	0	0	0
front-port 1/2	0	0	0	0
front-port 1/3	0	0	0	0
front-port 1/4	0	0	0	0
front-port 1/5	0	0	0	0
Port	UC sent	MC sent	BC sent	Octets sent
-----	-----	-----	-----	-----
-				
front-port 1/0	25710	3426	18	2523658
front-port 1/1	0	0	0	0
front-port 1/2	0	0	0	0
front-port 1/3	0	0	0	0
front-port 1/4	0	0	0	0
front-port 1/5	0	0	0	0

Step 2. For detailed statistics, use the **show interface <id> counters detail** command:

```
ma4000# show interface front-port 1/0 counters detail
```

Counter	Value
-----	-----
UC sent	127
MC sent	13
BC sent	8
Octets sent	11899
UC recv	182
MC recv	131
BC recv	50
Octets recv	40473
Bad octets recv	0
MAC transmit err	0
Bad frames recv	0
Frames 64 octets pass	47
Frames 65-127 octets pass	320
Frames 128-255 octets pass	142
Frames 256-511 octets pass	2
Frames 512-1023 octets pass	0
Frames 1024-max octets pass	0
Excessive collisions	0
Unrec MAC cntr recv	0
FC sent	0
Good fc recv	0
Drop events	0
Undersize packets	0
Fragments packets	0
Oversize packets	0
Jabber packets	0
MAC receive err	0
Bad CRC	0
Collisions	0
Late collisions	0
Bad FC recv	0
Current load Kbits sent/sec	1
Current load Kbits recv/sec	3
Current load frames sent/sec	2
Current load frames recv/sec	5
5:00 average Kbits sent/sec	0

```
5:00 average Kbits recv/sec      1
5:00 average frames sent/sec     0
5:00 average frames recv/sec     1
```

Step 3. To view the interface load, execute the **show interface <id> utilization** command: Command output shows the load for the last period, defined by the **load-average** command.

```
ma4000# show interface front-port 1/0 utilization

  Last utilization counters
  ~~~~~
Port          Kbits sent/sec    Kbits recv/sec    Frames sent/sec    Frames recv/sec
-----
front-port 1/0      2              3              3              5

  5m:00s utilization average
  ~~~~~
Port          Kbits sent/sec    Kbits recv/sec    Frames sent/sec    Frames recv/sec
-----
front-port 1/0      0              1              0              1
```

40.5 Interface Mirroring

Port mirroring allows to duplicate the traffic for monitored ports, sending inbound and/or outbound packets to the controlling port. Users can define controlled and controlling ports and select the type of traffic (inbound or outbound), that will be sent to the controlling port. In this example, all the traffic from the *slot-port 0* will be forwarded to the *front-port 1/5*, where it may be viewed using protocol analyzers (e.g. wireshark).

40.5.1 Controlled Port Configuration

Step 1. Define mirroring parameters for the inbound and outbound traffic.

```
ma4000# configure terminal
ma4000(config)# mirror rx interface slot-port 0
ma4000(config)# mirror tx interface slot-port 0
```

Step 2. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

40.5.2 Controlling Port Configuration

Step 1. Define traffic mirroring and analysis parameters for any **front-port**.

```
ma4000(config)# mirror rx analyzer front-port 1/5
ma4000(config)# mirror tx analyzer front-port 1/5
```

Step 2. Apply the configuration using the **commit** command.

```
ma4000(config)# do commit
```

41 PLC8 MONITORING

41.1 GPON OLT State

Step 1. To view GPON OLT state, use the **show slot <SLOT> gpon olt state** command.

```
ma4000(config)# do show slot 0 gpon olt state
Device count:          2
Channels per device:   4
Driver version:        1.2.561
Device 0:
  Firmware version:    2.3.37.1008
  Hardware version:    5211.2
Device 1:
  Firmware version:    2.3.37.1008
  Hardware version:    5211.2
```

Table 25 shows description of the displayed GPON OLT parameters.

Table 25—GPON OLT Parameters

Parameter	Description
Device count	The number of OLT chips
Channels per device	The number of channels in one OLT chip
Firmware version	OLT chip firmware version
Hardware version	OLT chip hardware version

41.2 GPON Interface State

Step 1. To view the state of GPON interfaces, use the **show interface gpon-port <SLOT>/0 - 7 state** command.

```
ma4000# show interface gpon-port 0/0-7 state
Channels status information:
Channel:          0      1      2      3      4      5      6      7
State:            OK     OK     OK     OK     OK     OK     OK     OK
ONT count:        0      0      0      0      0      0      0      0
SFP vendor:       Ligent  n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP product number:  LTE3680M-BC n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP vendor revision:  1.0    n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP temperature [C]:  53     n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP voltage [V]:     3.30   n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP tx bias current [mA]: 16.90  n/a    n/a    n/a    n/a    n/a    n/a    n/a
SFP tx power [dBm]:   3.35   n/a    n/a    n/a    n/a    n/a    n/a    n/a
```

Table 26—Parameters of GPON Interfaces

Parameter	Description
Channel	Channel number
State	Channel state
ONT count	The number of ONT in the channel
SFP vendor	SFP vendor
SFP product number	SFP model
SFP vendor revision	SFP revision
SFP temperature	SFP temperature in Celsius degrees

SFP voltage	SFP voltage in Volts
SFP tx bias current	Bias current in mA
SFP tx power	Transmission power in dBm

Table 27—States of GPON Interfaces

State	Description
INITED	Channel initialized
CFGINPROGRESS	The channel configuration is in progress
CFGFAILED	The channel configuration completed with error
OK	The channel is in operation
FAILED	The channel is out of operation
DISABLED	The channel is disabled

Step 2. To view the state of only GPON interface, execute the **show interface gpon-port <SLOT>/<ID> state** command.

```
ma4000# show interface gpon-port 0/0 state
Channel status information:
Channel: 0
State: OK
ONT count: 0
SFP vendor: Ligent
SFP product number: LTE3680M-BC
SFP vendor revision: 1.0
SFP temperature [C]: 47
SFP voltage [V]: 3.30
SFP tx bias current [mA]: 16.16
SFP tx power [dBm]: 3.41
```

41.3 MAC Table Preview

Step 1. To view the table of MAC addresses on the 2nd GPON interfaces slot 0 , execute the **show mac interface gpon-port 0/2** command.

```
ma4000# show mac interface gpon-port 0/2
Mac table
~~~~~
##      ONT Serial      ONT ID  GPON-port  GEM  UVID  CVID  SVID  MAC
--      -
1  454C54581A000035    40      2      640  10   302  1105  A8:F9:4B:5A:BD:15
2  454C54581A000035    40      2      643  9    9    1105  A8:F9:4B:5A:BD:14
3  454C54581C002D0A    35      2      603  9    9    1105  A8:F9:4B:71:66:49
4  454C54585C0104B0    39      2      635  9    9    1105  A8:F9:4B:C2:30:BA
5  454C54581A025A1F    63      2      825  12   305  1105  A8:F9:4B:6E:A4:02
6  454C54585F000010    38      2      627  9    9    1105  A8:F9:4B:C0:00:59
7  454C54581A025A1F    63      2      827  9    9    1105  A8:F9:4B:6E:A4:00
8  454C54581A025A1F    63      2      824  10   305  1105  A8:F9:4B:6E:A4:01

8 valid mac entries
```

41.4 Statistics for GPON Interfaces

Step 1. To view statistics of GPON interfaces, execute the **show interface gpon-port counters** command.

```
show interface gpon-port 0/0-7 counters
```

##	Downstream counters for channels:	0	1	2
...				
2	RX DS octets	1627665	1627665	1627665
3	RX DS packets	21044	21044	21044
5	RX DS octets for channel	1627665	0	0
6	RX DS packets for channel	21044	0	0
8	TX DS octets	13585411	0	0
9	TX DS packets	266867	0	0
11	DS octets	1422563	0	0
12	DS packets	20261	0	0
13	DS unicast packets	18424	0	0
14	DS multicast packets	958	0	0
15	DS broadcast packets	879	0	0
16	DS packet dropped	383	0	0
##	Upstream counters for channels:	0	1	2
2	TX US octets	1704580	0	0
3	TX US packets	19966	0	0
5	US octets	1457760	0	0
6	US packets	19560	0	0
7	US unicast packets	18709	0	0
8	US multicast packets	400	0	0
9	US broadcast packets	451	0	0
10	US packet dropped	50	0	0
11	Packet dropped (CRC)	0	0	0
13	TX US octets reassembly	17909382	0	0
14	TX US packets reassembly	265915	0	0

41.5 Statistics for OLT V Interfaces

Step 1. To view statistics of OLT V interfaces (ethernet interfaces that are connected to a switch interface module), execute the **show interface gpon-port <SLOT>/0-7 counters v-interface** command.

```
ma4000# show interface gpon-port 0/0-7 counters v-interface
```

##	Downstream counters for channels:	0	1	2	3	4	5	6	7
1	RX Alignment errors	0	0	0	0	0	0	0	0
2	RX Pause frames	0	0	0	0	0	0	0	0
3	RX CRC-32 errors	0	0	0	0	0	0	0	0
4	RX Oversize errors	0	0	0	0	0	0	0	0
5	RX Bad FCS	0	0	0	0	0	0	0	0
6	RX Too long frames	0	0	0	0	0	0	0	0
7	RX Undersize errors	0	0	0	0	0	0	0	0
8	RX Range errors	0	0	0	0	0	0	0	0
9	RX Ok frames	21229	0	0	0	2	0	0	0
10	RX total frames	21229	0	0	0	2	0	0	0
11	RX 64 octets frames	0	0	0	0	0	0	0	0
12	RX 65-127 octets frames	20715	0	0	0	2	0	0	0
13	RX 128-255 octets frames	65	0	0	0	0	0	0	0
14	RX 256-511 octets frames	404	0	0	0	0	0	0	0
15	RX 512-1023 octets frames	42	0	0	0	0	0	0	0
16	RX 1024-1518 octets frames	3	0	0	0	0	0	0	0
17	RX 1519-MAX octets frames	0	0	0	0	0	0	0	0
18	RX Total unicast packets	18994	0	0	0	0	0	0	0
19	RX Total multicast packets	966	0	0	0	0	0	0	0
20	RX Total broadcast packets	1269	0	0	0	2	0	0	0
22	RX Total octets	1641763	0	0	0	152	0	0	0

24	RX Ok octets	1641763	0	0	0	152	0	0	0
25	RX FIFO overflow errors	0	0	0	0	0	0	0	0
26	RX Bad FCS and <64 octets	0	0	0	0	0	0	0	0
27	RX Frame errors	0	0	0	0	0	0	0	0
##	Upstream counters for channels:	0	1	2	3	4	5	6	7
1	TX frames without errors	20146	0	0	0	0	0	0	0
2	TX valid pause frames	0	0	0	0	0	0	0	0
3	TX frames with errors	0	0	0	0	0	0	0	0
4	TX good unicast packets	19274	0	0	0	0	0	0	0
5	TX good multicast packets	404	0	0	0	0	0	0	0
6	TX good broadcast packets	468	0	0	0	0	0	0	0
8	TX octets	1719437	0	0	0	0	0	0	0

41.6 Multicast Statistics

Step 1. To view statistics of MC flows, execute the **show interface gpon-port <SLOT>/<PORT> igmp groups** command. As a parameter, pass the channel number.

```
ma4000# show interface gpon-port 0/0 igmp groups
```

All IGMP groups (4):

#	Channel	Serial	Multicast address	Start	Stop
1	0	ELTX1A025A08	239.255.255.250	2014.04.17 13:54:54	2014.04.17 14:22:07
2	0	ELTX1A025A08	239.255.255.250	2014.04.17 14:26:06	2014.04.17 14:32:48
3	0	ELTX1A025A08	239.255.255.250	2014.04.17 14:36:35	2014.04.17 14:42:53
4	0	ELTX1A025A08	239.255.255.250	2014.04.17 14:46:57	2014.04.17 15:37:05

42 ONT MONITORING

42.1 ONT Configurations List

Step 1. To view ONT active configurations, execute the **show interface ont <SLOT>/<PORT> configured** command.

```
ma4000# show interface ont 0/0 configured

-----
Slot 0 GPON-port 0 ONT configured list
-----

  ##              Serial          ONT ID   Assigned channel   Description
  1              0000000000000000         0           0
Slot 0 total ONT count: 1
```

42.2 Active ONT List

Step 1. To view ONT empty configurations, execute the **show interface ont <SLOT>/<PORT> unconfigured** command.

```
ma4000# show interface ont 0/0 unconfigured

Slot 0 GPON-port 0 has no unconfigured ONTs
Slot 0 total ONT count: 0
```

42.3 Online ONT List

Step 1. To view online ONT list, execute the **show interface ont <SLOT>/<PORT> online** command.

```
ma4000# show interface ont 0-15/0-7 online

Slot 0 GPON-port 0 has no online ONTs
Slot 0 GPON-port 1 has no online ONTs
Slot 0 GPON-port 2 has no online ONTs
Slot 0 GPON-port 3 has no online ONTs
Slot 0 GPON-port 4 has no online ONTs
Slot 0 GPON-port 5 has no online ONTs
Slot 0 GPON-port 6 has no online ONTs
Slot 0 GPON-port 7 has no online ONTs

Slot 0 total ONT count: 0
```

Table 28—Description of ONT States

ONT State	Description
UNACTIVATED	ONT has no configurations
ALLOCATED	ONT detected
AUTHINPROGRESS	ONT authentication is in progress
AUTHFAILED	Authentication failed
AUTHOK	Authentication successfully completed

PRECONFIG	Preparing ONT for configuration
CFGINPROGRESS	ONT configuration is in progress
CFGFAILED	Configuration failed
OK	ONT is in operation
BLOCKED	ONT is blocked
MIBRESET	ONT MIB reset
FAILED	ONT has a critical failure
FWUPDATING	ONT firmware update is in progress
DISABLED	ONT is disabled (technically blocked)

42.4 Offline ONT List

Step 1. To view the list of disconnected ONTs, execute the **show interface ont <SLOT>/<PORT> offline** command.

```
ma4000# show interface ont 0-15/0-7 offline

-----
Slot 0 GPON-port 0 ONT offline list
-----

  ##              Serial          ONT ID   Assigned channel   Description
  1              0000000000000000         0             0
Slot 0 GPON-port 1 has no offline ONTs
Slot 0 GPON-port 2 has no offline ONTs
Slot 0 GPON-port 3 has no offline ONTs
Slot 0 GPON-port 4 has no offline ONTs
Slot 0 GPON-port 5 has no offline ONTs
Slot 0 GPON-port 6 has no offline ONTs
Slot 0 GPON-port 7 has no offline ONTs
Slot 0 total ONT count: 1
```

42.5 ONT Statistics

To view ONT statistics, use the **show interface ont <SLOT>/<PORT>/<ID> counters** command. Pass the number of requested statistical data (see Table 29) and ONT ID as parameters.

```
ma4000# show interface ont 0/0/0 counters gem-port-nctp-performance-monitoring

-----
[ONT0/0/0] counters
-----

  ##   Downstream counters for cross-connects:   0    1    ...    7    MC    BC
  1   Finished intervals                        23   ---   ...   ---   ---   23
  2   Received GEM frames                       0   ---   ...   ---   ---   0
  4   Received payload bytes                    0   ---   ...   ---   ---   0

  ##   Upstream counters for cross-connects:     0    1    ...    7    MC    BC
  1   Finished intervals                        23   ---   ...   ---   ---   23
  2   Transmitted GEM frames                    0   ---   ...   ---   ---   0
  4   Transmitted payload bytes                  0   ---   ...   ---   ---   0
```

Table 29—ONT Statistical Data Types

Type of statistics	Description	Scope
cross-connect	GEM port statistics	OLT
gem-port-performance-monitoring	GEM port statistics	ONT
gem-port-nctp-performance-monitoring	GEM port statistics	ONT
ethernet-performance-monitoring-history-data	ETH port statistics (G.984.4)	ONT
ethernet-performance-monitoring-history-data2	ETH port statistics (G.984.4)	ONT
ethernet-performance-monitoring-history-data3	ETH port statistics (G.984.4)	ONT
gal-ethernet-performance-monitoring-history-data	Statistics transition GEM in ETH	ONT
fec-performance-monitoring-history-data	Statistics redundant coding	ONT
ethernet-frame-extended-performance-monitoring	ETH port statistics (G.988)	ONT
multicast-subscriber-monitor	Multicast statistics	ONT

42.6 ONT Bit Error Rate



Bit error rate (BER) is the rate of errors in data transmission.

To view BER on example of ONT, execute the **show interface gpon-port <slot>/<port> downstream-ber** command. As a parameter, pass the number of the GPON interface.

```
ma4000# show interface ont 0-15/0-7 downstream-ber
```

```
-----
Slot 0 GPON-port 0 BER table
-----
    No records
-----
Slot 0 GPON-port 1 BER table
-----
    No records
-----
Slot 0 GPON-port 2 BER table
-----
    No records
-----
Slot 0 GPON-port 3 BER table
-----
    No records
-----
Slot 0 GPON-port 4 BER table
-----
    No records
-----
Slot 0 GPON-port 5 BER table
-----
    No records
-----
Slot 0 GPON-port 6 BER table
-----
    No records
-----
Slot 0 GPON-port 7 BER table
-----
    No records
```

PART VI

MAINTENANCE

43 REPLACEMENT OF PWR IN POWER INPUT MODULES

This Chapter describes the replacement procedure for one of the PWR IN power input modules without actual shutdown of the access node.

Step 1. Use the **show system environment** command to ensure that the power supply is present on both feeders.

```
ma4000# show system environment
MFC board status:      ok
MFC board version:     0x2
MFC firmware:
  Status:              0x00 (ok)
  Version:             8 2 1 1 5 05/11/2013
  Timestamp (UTC):     05-Nov-2013 12:19:22

Fan configured speed, %: auto
Fan current speed, %:  57
Fan minimum speed, %:  15
Fan speed levels, %:   15 25 36 46 57 68 78 89 100

                        Fan0      Fan1      Fan2
Status:                ok        ok        ok
RPM:                   1824      1818      1860

                        Feeder1   Feeder2
Status:                ok        ok
Current, A:            0.52      1.00
Voltage, V:            -51.25    -53.75

Shelf voltage, V:      -54.28
```

Step 2. Disable the power supply on one of the feeders using the power distribution device (depends on the project).

Step 3. Use the voltmeter gauge to make sure, that there is no voltage on the input terminals of the **PWR IN** power input module.

Step 4. Disconnect cables from the power module input terminals.

Step 5. Remove the screw that holds the power input module in the crate. Pull out the module bracket and remove it from the crate.

Step 6. Install a new **PWR IN** power input module into the crate. Fasten the screw that holds the power input module in the crate.

Step 7. Connect cables to the input terminals of the power module observing correct polarity.

Step 8. Power up the disabled feeder.

Step 9. Use the **show system environment** command to ensure that the power supply is present on both feeders.

44 REPLACEMENT OF MFC MODULE

You can replace the MFC module without actual shutdown of the access node.

Step 1. Remove the screw that holds the **MFC** module in the crate.

Step 2. Pull out the module bracket and remove it from the crate. Fans will switch to maximum performance mode.

Step 3. Install a new **MFC** module into the crate. Fasten the screw that holds the MFC module in the crate.

Step 4. Use the **show system environment** command to ensure that the new module has been successfully identified by the system. Fans will switch to normal performance mode.

```
ma4000# show system environment
MFC board status:      ok
MFC board version:     0x2
MFC firmware:
  Status:              0x00 (ok)
  Version:             8 2 1 1 5 05/11/2013
  Timestamp (UTC):     05-Nov-2013 12:19:22

Fan configured speed, %: auto
Fan current speed, %:  57
Fan minimum speed, %:  15
Fan speed levels, %:   15 25 36 46 57 68 78 89 100

                        Fan0      Fan1      Fan2
Status:                ok        ok        ok
RPM:                   1824      1818      1860

                        Feeder1   Feeder2
Status:                ok        ok
Current, A:            0.52      1.00
Voltage, V:            -51.25    -53.75
Shelf voltage, V:      -54.28
```

45 REPLACEMENT OF PP4X CENTRAL SWITCH MODULES

You can replace PP4X modules without actual shutdown of the access node only when there are two PP4X modules installed in the rack.

Step 1. If the module to be replaced is the master module, you should change the master for this access node.

```
ma4000# stack master change
```

Step 2. Make sure, that the master has been changed successfully for this access node:

```
ma4000# show stack
Stack Units
~~~~~
Unit   Position  Role    Prio  MAC Address          Version          Sync
----   -
*1     Left      BACKUP  240   22:22:22:22:22:22    1 1 8 0 21501    Enabled
2      Right    MASTER  208   00:48:43:ef:c0:56    1 1 8 0 21501    Enabled

Stack-channel State
~~~~~
Interface          Status
-----
stack-port 1/0      up
stack-port 1/1      up
```

Also, you may check the 'Master' LED indicator on the PP4X front panel—it should be solid green.

Step 3. Disconnect all optical and electric patch cords from the module to be replaced. Also, make sure to protect the connectors with the dust caps.

Step 4. Remove all SFP transceivers from the PP4X module. SFP transceiver removal procedure is described in details in [47 SFP Transceivers Replacement](#).

Step 5. Remove the screws located on the module ejectors. Push the bottom ejector down and pull the top ejector up. Pull out the module and remove it from the crate, Fig. 45.

Step 6. Install a new PP4X module in reversed order, Fig. 45.



To prevent the board damage, install/remove boards to/from the crate carefully, do not apply any force.

Do not allow the components of the board being installed to touch the board installed next to it. If the board meets resistance while sliding through the guides, remove the board and try to install it again.

After all modules has been installed into the rack, secure the connection with screws, see Fig. 45.

Step 7. Install SFP transceivers back into the PP4X module. SFP transceiver installation procedure is described in details in [47 SFP Transceivers Replacement](#).

Step 8. Reconnect optical and electric patch cords according to the wiring documentation.

Step 9. Check the state of PP4X module using the **show stack** command.

Step 10. If necessary, change the master module back with the **stack master change** command.

46 REPLACEMENT OF PLC8 GPON INTERFACE MODULES

You can replace the PLC8 modules without actual shutdown of the access node.

Step 1. Disconnect all optical patch cords from the module to be replaced. Also, make sure to protect the connectors with the dust caps.

Step 2. Remove all SFP transceivers from the PLC8 module. SFP transceiver removal procedure is described in details in Section [47 SFP Transceivers Replacement](#).

Step 3. Remove the screws located on the module ejectors. Push the bottom ejector down and pull the top ejector up. Pull out the module and remove it from the crate, Fig. 45.

Step 4. Install a new PLC8 module in reversed order, Fig. 45.

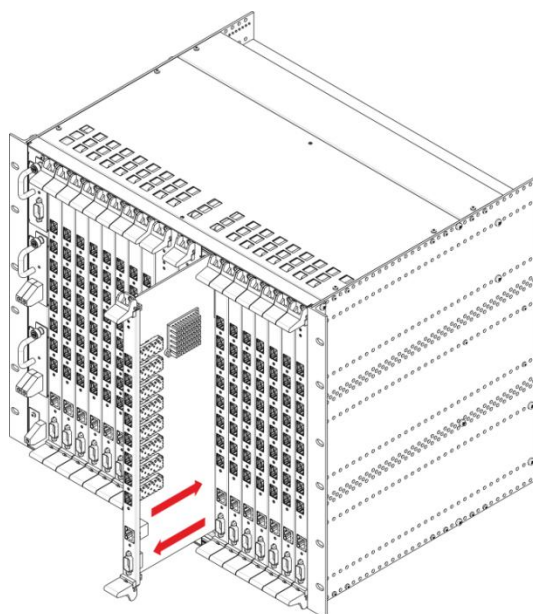


Fig. 45—Installing board into MA4000-PX



To prevent the board damage, install/remove boards to/from the crate carefully, do not apply any force. Do not allow the components of the board being installed to touch the board installed next to it. If the board meets resistance while sliding through the guides, remove the board and try to install it again. After all modules has been installed into the rack, secure the connection with screws, see Fig. 45.

Step 5. Install SFP transceivers back into the PLC8 module. SFP transceiver installation procedure is described in details in Section [47 SFP Transceivers Replacement](#).

Step 6. Reconnect optical patch cords according to the wiring documentation.

Step 7. Check the state of PLC8 module using the **show slots** command. Replaced module should be in the **Operational** state.

```
ma4000# show slots
```

```
Shelf status
```

```
~~~~~
```

Slot #	Configured Type	Detected Type	Version	Serial #	Link State	Slot State
-----	-----	-----	-----	-----	-----	-----
-						
0	plc8	plc8	3.22.0.244	OL04001750	up	Operational
1	none	none	0.0.0.0		down	Absent
2	none	none	0.0.0.0		down	Absent
3	none	none	0.0.0.0		down	Absent
4	none	none	0.0.0.0		down	Absent
5	none	none	0.0.0.0		down	Absent
6	none	none	0.0.0.0		down	Absent
7	none	none	0.0.0.0		down	Absent
8	none	none	0.0.0.0		down	Absent
9	none	none	0.0.0.0		down	Absent
10	none	none	0.0.0.0		down	Absent
11	none	none	0.0.0.0		down	Absent
12	none	none	0.0.0.0		down	Absent
13	none	none	0.0.0.0		down	Absent
14	none	none	0.0.0.0		down	Absent
15	none	none	0.0.0.0		down	Absent

47 SFP TRANSCEIVERS REPLACEMENT

SFP transceivers can be installed when the access node is turned on or off.

Step 1. Insert an SFP transceiver into a slot. SFP transceivers are set as shown in Fig. 46.

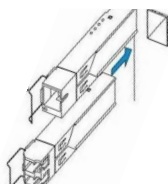


Fig. 46—SFP Transceivers Installation

Step 2. Press the module until it fits with a click.



Fig. 47—Installed SFP Transceivers

To remove a transceiver, perform the following actions:

Step 1. Unlock the module's latch.



Fig. 48—Opening the Latch of SFP Transceivers

Step 2. Remove the module from the slot.

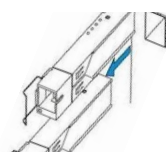


Fig. 49—Removing SFP Transceivers

48 PP4X FIRMWARE UPDATE

48.1 Firmware Update via CLI

48.1.1 Introduction

Firmware files are stored in the non-volatile memory (flash memory).

The flash memory can store up to two firmware files simultaneously. The first file is active and used at the device startup. The second file is a backup file. Storing two firmware files in flash memory allows to protect the device, if one of the files becomes corrupted for some reason.

Another active file can be chosen in the following circumstances:

- When the active firmware file corruption is detected
- On the operator's command
- When the device firmware update is performed
- When the automatic roll back to the previous version of the firmware is activated

To use the newest firmware version:

1. Copy the new device firmware file into the device flash memory
2. Set this file as active firmware file
3. Reboot the device

Use CLI commands to perform these operations.

48.1.2 New firmware version installation procedure



If there are two devices installed in a rack, we strongly recommend to use the same firmware version on both devices. This way you will be able to perform the firmware update simultaneously on both devices.

Firmware update procedure:

Step 1. Copy the firmware file located on the external TFTP server into the flash memory of the device using the **copy**¹ command.

Command format: `copy tftp://<ip>/<path> fs://firmware`

where

- <ip>—TFTP server IP address
- <path>—path to the file on TFTP server

¹ Basic level command (ROOT), help string appearance: ma4000#

Step 2. Set the inactive firmware file as active using the **firmware select image-alternate unit**¹ command:

Command format: **firmware select image-alternate unit <unit>**

where <unit> is the PP4X module number; possible values [1-2].

If the firmware file has been copied into the flash memory of both devices at Step 1, you have to enter this command twice and pass numeric values '1' or '2' as the <unit> parameter.

Step 3. Reboot devices with updated firmware:

- a. If the firmware has been updated on both devices, enter the **reboot system**¹ command.
- b. If the firmware has been updated only on one of the devices and this device is the stack master, enter the **reboot master**¹ command.
- c. If the firmware has been updated only on one of the devices and this device is the stack slave, enter the **reboot slave**¹ command.

You may also use the **reboot system** command for cases 'b' and 'c'. However, note that the **reboot system** command reboots the entire device.

Step 4. Make sure that the new firmware version is working correctly after devices' startup.

Use the **show firmware**¹ command to check the state of the firmware file installed during Steps 1-3—it should read 'TESTING'.

```
MA4000# show firmware
```

Firmware status:					
~~~~~					
Unit	Image	Running	Boot	Version	Date
----	-----	-----	-----	-----	-----
-					
1	0	No	FALLBACK*	1 3 2 267 40378	03-Oct-2014 20:10:03
1	1	Yes	TESTING	1 3 2 323 40564	20-Oct-2014 20:12:02
2	0	Yes	TESTING	1 3 2 323 40564	20-Oct-2014 20:12:02
2	1	No	FALLBACK*	1 3 2 267 40378	03-Oct-2014 20:10:03

"*" designates that the image was selected for the next boot

```
MA4000#
```

4. Confirm the successful completion of the firmware update with the **firmware confirm** command:¹

Command format: **firmware confirm**

¹ Basic level command (ROOT), help string appearance: ma4000#



If the device has the new firmware version installed and the 'firmware confirm' command is not executed within 5 minutes after its startup, the device will be automatically rebooted. At that, the active firmware file (new firmware version) will be marked as inactive by the bootloader and the active firmware file (previous firmware version) will be marked as active. After that, the active firmware file will be loaded.

### 48.1.3 Examples of the new firmware version installation procedure

Source data:

- Firmware file is located on the TFTP server
- TFTP server IP address 192.168.0.100
- path to the firmware file on TFTP server: pp4x/firmware.pp4x
- firmware update is required for devices with stack numbers 1 and 2

1. Copy the firmware file located on the external TFTP server into the flash memory of both devices.

```
copy tftp://192.168.0.100/pp4x/firmware.pp4x fs://firmware
```

2. Configure the inactive firmware file as active.

```
ma4000# firmware select image-alternate unit 1
ma4000# firmware select image-alternate unit 2
```

3. Reboot devices with updated firmware. Firmware update has been performed on both devices, thus you should reboot both devices:

```
ma4000# reboot system
```

4. Make sure, that the firmware update has been completed successfully. Check contents of devices' flash memory:

```
MA4000# show firmware

Firmware status:
~~~~~
Unit Image Running Boot Version Date

1 0 No * 1 3 2 267 40378 03-Oct-2014 20:10:03
1 1 Yes * 1 3 2 323 40564 20-Oct-2014 20:12:02
2 0 Yes * 1 3 2 323 40564 20-Oct-2014 20:12:02
2 1 No * 1 3 2 267 40378 03-Oct-2014 20:10:03

"*" designates that the image was selected for the next bootMA4000#
```

5. Confirm, that the firmware update has been completed successfully.

```
ma4000# firmware confirm
```

## 48.2 Firmware Update via Bootloader (U-Boot)

As a rule, firmware update is performed through the command line interface (CLI), provided by means of the device firmware.

If necessary, you can update the firmware via the command line interface, provided by means of the bootloader.

### 48.2.1 Firmware Update via Bootloader

1. Connect the device (through the CONSOLE port) to PC with RS-232 (DB-9F) cable.
2. Connect the device (one of the ports 0-5) to the TFTP server or the router, that will establish connection to TFTP server.
3. Run terminal emulation application on PC (HyperTerminal, TeraTerm) and perform the following actions:
  - a. Select the corresponding serial port.
  - b. Set the data transfer rate—115,200 baud.
  - c. Specify the data format: 8 data bits, 1 stop bit, non-parity.
  - d. Disable hardware and software data flow control.
4. Turn the device on. Wait until the text *"Autobooting in 3 seconds, press 'stop' for stop"* appears on the PC screen. Enter the **stop** command. Make sure, that the command prompt is displayed on the screen ('PP4X>').
5. Define TFTP server IP address:

```
set serverip <IP-addr>
```

6. Define the device IP address:

```
set ipaddr <IP-addr>
```



**Default IP address of the device is 192.168.0.2**

7. Define the gateway IP address for access to TFTP server. If the device IP address and TFTP server IP address belong to different subnets:

```
set gatewayip <IP-addr>
```

8. Make sure, that the device is successfully connected to TFTP server.

```
ping <IP-addr TFTP-server>
```

9. If the connection was successful, you will see the following message:

```
host <IP-addr TFTP-server> is alive
```

10. If there is no connection, you will see the following message:

```
ping failed; host <IP-addr TFTP-server> is not alive
```



Depending on the IP filtering settings of TFTP server, gateway or intermediate routers, connection test may result in 'ping failed' message, regardless of a working connection between TFTP server and the device.

11. Set the path to the firmware file on TFTP sever:

```
set fw_name <path>
```

By default, path to the firmware file on TFTP sever appears as follows: **pp4x/firmware.pp4x**.

12. Copy the firmware file from TFTP server to the device flash memory and mark the firmware file as active:

```
run upgrade
```

13. Wait until 'run upgrade' command finishes ('PP4X>' will appear).



**Command execution time is approximately 90 seconds.**

14. Make sure, that the following messages were shown during the **run upgrade** command execution:

```
2 of 2 kernel images successfully installed
2 of 2 filesystem images successfully installed
Firmware installation finished.
```

15. Reboot the device:

```
reset
```

16. Wait until the device startup procedure finishes. Log in (enter user name and password).



**If the device configuration matches the default configuration, you can log in with the user name 'admin' and the password 'password'.**

17. Make sure, that the required firmware version is located in the device flash memory and defined as active, using the **show firmware** command.

## 48.2.2 Possible Abnormal Situations During the Firmware Upgrade via Bootloader

1. The following message appears when the **run upgrade** command is entered:

```
Loading: T T T T T T T T T T
Retry count exceeded; starting again
```

**Reason:** TFTP server is not available.

**Solution:** Make sure, that TFTP server or intermediate equipment, such as routers, are configured and operating properly. Abort the **run upgrade** command execution; press <Ctrl+C>. Check, if 'serverip', 'ipaddr', 'gatewayip' parameters are defined correctly. Retry the **run upgrade** command execution.

2. The following message appears when the **run upgrade** command is entered:

```
ERROR: installing new firmware is allowed only in CURRENT state.
Type "image rollback" to switch to CURRENT state.
```

**Reason:** Firmware update attempt using the **boot system** command was taken earlier. At that, the 'confirmed' parameter has been specified, that matches the firmware update mode with the user confirmation request ('boot confirm') after the reboot.

Error message means that the reboot was not performed after the **boot system** command entry or that the confirmation was not received ('boot confirm').

**Solution:** Enter the **image rollback** command. Roll back to the previous firmware version will be performed: the active firmware file will be marked as inactive, and the inactive firmware file will be marked as active. After that, retry the **run upgrade** command execution.

## 49 EMERGENCY RECOVERY OF PP4X FIRMWARE

After the user has specified the file with new firmware version as the active file and executed the device reboot command, the device will be loaded with the new firmware version. If you experience problems while operating with the new firmware version, you can use automatic rollback procedure, that allows you to restore the previous firmware version.

When device starts up with the new firmware version, it waits for the firmware update confirmation from the user with the following command: **firmware confirm**¹.

If the confirmation is not provided within 5 minutes after the device startup, it will be rebooted automatically, and will be rolled back to the previous firmware version on the next startup:



**If the device operation is interrupted before executing the confirmation command (*firmware confirm*¹), the device will be rolled back to the previous firmware version on the next startup.**

**Device operation may be interrupted for one of the following reasons:**

- **User has executed the device reboot command**
- **Device power supply has been switched off**
- **Device has performed an emergency reboot**

---

¹ Basic level command (ROOT), help string appearance: ma4000#



## 50 ONT FIRMWARE UPDATE

### 50.1 Introduction

This Chapter describes different methods of ONT firmware update using the OMCI protocol.

### 50.2 Overview

Fig. 50 shows the ONT firmware update infrastructure.

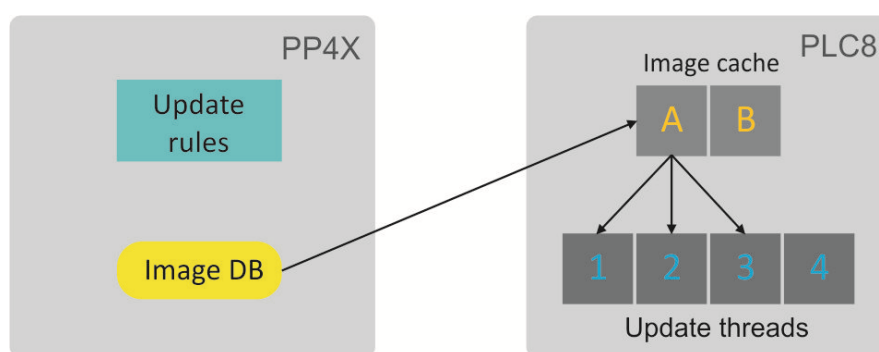


Fig. 50—ONT firmware update infrastructure

The 128 MB ONT firmware files storage is located at PP4X module. The maximum size of an ONT firmware file is 24 MB. When a file is stored in the storage, it can be used by PLC8 modules. See chapter [50.3 ONT Firmware Files Management](#) for detailed description of file management schemes for ONT firmware.

At the start of the ONT firmware update the firmware file is copied to the cache of PLC8 module. This takes about 1–2 minutes. Then an update stream transfers the file to ONT in small parts via OMCI. File transfer takes more time—usually about 10 minutes for a 16 MB file with window size of 96 kB. Thus, the firmware update for an ONT may totally take up to 12 minutes.

When the update is completed, the update file is not removed from the cache and can be used again later. This reduces the time required for further updates. However, the file can be replaced when both caches are full and a new firmware file should be used. To be replaced, the file should not be used by any update streams. If there are no unused files, the update operation will be put in a queue. It means that up to 4 ONTs with different firmware files can be simultaneously updated for each PLC8 module.

An access node can also update ONT firmware automatically. To control the mode, the following settings are provided. See section [50.5 Configuration of ONT Firmware Auto Update](#) for description. There are two ONT auto update modes.

The immediate mode allows all ONTs to be updated within the shortest possible time because they are updated one by one. The mode's disadvantage is the necessary ONT reboot after activation of a new firmware image and, consequently, possible interruptions in operation of services.

The postpone mode is more delicate: a new update is performed only after the previously updated ONT firmware has been activated. User does not encounter any occasional difficulties with services operation. This mode may take more time to update all ONTs.

A decision to launch ONT update is made based on auto update rules. Every auto update rule contains the following information:

- unique rule name, which allows rule modification;
- ONT type (the Equipment-ID field);
- firmware version¹, which indicates that the firmware should be updated;
- name of the file from the ONT firmware files storage that should be used for update;
- rule scope: global or local.

ONT firmware auto update can be activated/deactivated based on global or local rules. For more details on auto update rules see section [50.5.2 ONT Auto Update Rules](#).

## 50.3 ONT Firmware Files Management

In order to download an ONT firmware file, the **copy** command is used with the file's name and address of a TFTP server:

```
ma4000# copy tftp://192.168.1.100/ntp-rg-d3.20.2.169.fw.bin fs://ont-firmware
Download file from TFTP-server..
.....
ONT firmware vendor is Eltex Corporation, version 3.20.2.169 Write downloaded
file to flash memory..
.....
```

Being downloaded, the ONT firmware file is moved to ONT firmware files storage in PP4X and can be used by PLC8 modules.

Use the **show firmware ont** command to view the content of the ONT firmware files storage in PP4X:

```
ma4000# show firmware ont
ONT firmware images:
~~~~~
```

#	Filename	Version	Hardware
1	ntp-rg-revb-d3.20.2.174.fw.bin		
2	ntp-rg-revb-d3.20.2.170.fw.bin		
3	ntp-rg-d3.20.2.169.fw.bin		
4	ntp-rg-d3.20.2.165.fw.bin		

To remove a firmware file, use the **firmware ont delete image** command with the file's name:

```
ma4000# firmware ont delete image ntp-rg-d3.20.2.165.fw.bin
Firmware deleting finished.
```

¹ The field containing information about firmware version allows negation, i. e. the use of the prefix "!". This allows complex rules as: if firmware version is not equal 1.2.3, use the 1_2_3.bin file for update.

## 50.4 ONT Firmware Manual Update

This method is used to update the ONTs which are activated at the time of update.

To perform a forced update of an ONT, use the **update ont** command with the ONT's ID and name of the ONT firmware file available in PP4X storages:

```
ma4000# update ont 0/0 ntp-rg-r3.20.2.123.fw.bin
Task for updated successfully created. ONT firmware will be updated in 20 minutes
or more
```

A task will be created to update the ONT firmware with the specified ID. The task will end with an error for ONTs which are not connected.

## 50.5 Configuration of ONT Firmware Auto Update

### 50.5.1 ONT Auto Update Modes

ONT auto update has two modes: immediate and postpone.

Step 1. Activate the update mode by the **firmware ont auto update** command:

```
ma4000# firmware ont auto update postpone
```

Step 2. Apply the changes by using the **commit** command:

```
ma4000# commit
```

You can view the configured mode with the help of the **show firmware ont auto update state** command:

```
ma4000# show firmware ont auto update state
Auto-update ONT: postpone
```

Step 3. To disable the ONT firmware auto update, use the **no firmware ont auto update enable** command:

```
ma4000# no firmware ont auto update enable
```

### 50.5.2 ONT Auto Update Rules

Step 1. Use the **firmware ont auto update add** command to add a new auto update rule. Specify the rule's unique name, ONT type (Equipment-ID), firmware version to be updated, name of the file in the ONT firmware files storage to be used in the update, and the mode as parameters:

```
ma4000# firmware ont auto update add name2 NTP-RG 1.1.1 filename global
```

Step 2. To display the list of auto update rules, use the **show firmware ont auto update entries** command:

```
ma4000# show firmware ont auto update entries

Description  EquipmentID  FWVersion  FileName  Mode
Rule1|NTP-RG-1402G-W|3.20.2.123|ntp-rg-d3.20.2.124.fw.bin|global
Rule2|NTP-RG-1402G-W|3.20.2.124|ntp-rg-d3.20.2.125.fw.bin|global
```

Step 3. Use the **firmware ont auto update delete** command to remove an auto update rule:

```
ma4000# firmware ont auto update delete Rule1
```

## TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9

Phone:

+7(727) 220-76-10

+7(727) 220-76-07

E-mail: [post@eltexalatau.kz](mailto:post@eltexalatau.kz)

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

<http://www.eltexalatau.kz/en/>