

Engineering Design Specification:

-

|  |  |
| --- | --- |
| **Project Number:** |  |
| **Project Name:** | - |
| **Project Type:** | RBS |
| **Status:** |  |
| **Priority:** |  |
| **CA Number:** |  |
| **CA Approval Date:** |  |
| **Related Document Number:** |  |
|  |  |
| **Target In Service Date:** |  |
| **Regions Involved:** |  |
|  |  |
| **Revision Number:** |  |
| **Revision Date:** |  |
| **Original Release Date:** |  |
|  |  |
| **Prepared By:** |  |
| **Department:** |  |
| **Contributors:** |  |
| **Documentation Supported By:** |  |
| **Checked By:** |  |
| **Authorized By:** |  |
| **Distributed To:** | #RCI\_ENTERPRISE\_NETOPS\_PROJECTS  #RCS\_IPCORE\_PROJECTS  #Equipment Engineering Wireline  Ishfaq malik  Luisa Rondinone |
|  |  |

|  |
| --- |
| The information in this document is the property of Rogers Communication Partnership. The receiver of this document shall keep the information contained herein confidential and shall protect the same in whole or in part from disclosure and dissemination to third parties. Disclosure and disseminations shall only be made on a strict need to know basis and upon the consent of the author. |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Date** | **Revision** | **Author** | **Reason for Revision** |
|  |  |  | Original/Initial Release of document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1.0 Executive Summary 1](#_Toc85536750)

[2.0 Scope Section 1](#_Toc85536751)

[2.1 Scope of Work 1](#_Toc85536752)

[2.2 Benefit to the company 1](#_Toc85536753)

[2.3 Consequences if not done 1](#_Toc85536754)

[2.4 Measurement Criteria 1](#_Toc85536755)

[2.5 Acceptance Summary Checklist 1](#_Toc85536756)

[3.0 Financial Section 1](#_Toc85536757)

[3.1 General Information 1](#_Toc85536758)

[3.2 Inter-company/department Charges (if applicable) 1](#_Toc85536759)

[3.3 Bill of Materials 1](#_Toc85536760)

[3.4 OPEX 1](#_Toc85536761)

[4.0 Technical Section 1](#_Toc85536762)

[4.1 Solution Overview 1](#_Toc85536763)

[4.1.1 «Type7750» Install at «Address» 1](#_Toc85536764)

[4.1.2 Service Flow Diagram 1](#_Toc85536765)

[4.2 Platform Specifications 1](#_Toc85536766)

[4.2.1 Hardware Specifications 1](#_Toc85536767)

[4.2.2 Physical Installation 1](#_Toc85536768)

[4.2.3 Logical Network Connections 1](#_Toc85536769)

[4.2.4 Network Management 1](#_Toc85536770)

[4.2.5 Network Timing 1](#_Toc85536771)

[4.2.6 Operating System 1](#_Toc85536772)

[4.2.7 Initial Dimensioning 1](#_Toc85536773)

[4.2.8 Application Functional Specifications 1](#_Toc85536774)

[4.2.9 Service Redundancy and Failover Capabilities 1](#_Toc85536775)

[4.2.10 Support Services 1](#_Toc85536776)

[4.2.11 Performance and Fault Management 1](#_Toc85536777)

[4.2.12 Compliance 1](#_Toc85536778)

[4.3 Configuration Details 1](#_Toc85536779)

[4.3.1 Physical Installation of Alcatel-lucent 7750 SR12E 1](#_Toc85536780)

[Alcatel-lucent 7750 SR-12 Chassis Physical Overview 1](#_Toc85536781)

[4.3.2 Alcatel-lucent «Hardware7750» «Type7750» Hardware Layout 1](#_Toc85536782)

[4.4 End to End Impact Assessment 1](#_Toc85536783)

[4.4.1 Impact Classification 1](#_Toc85536784)

[4.4.2 Impacted Network Elements and Services and Locations 1](#_Toc85536785)

[4.4.3 Partial/Complete Quarantine on Network Elements/Region 1](#_Toc85536786)

[4.4.4 Teams Involved in the change implementation 1](#_Toc85536787)

[4.4.5 Changes to the existing IP and Service Flows 1](#_Toc85536788)

[4.4.6 Detailed Impact Assessment 1](#_Toc85536789)

[4.5 Technical Pre-requisites 1](#_Toc85536790)

[4.6 Technical Co-requisites 1](#_Toc85536791)

[4.7 Potential CBU Impacts/Risks 1](#_Toc85536792)

[4.8 IP Flow -- Security 1](#_Toc85536793)

[4.8.1 Network Security 1](#_Toc85536794)

[4.8.2 System Classifications 1](#_Toc85536795)

[4.8.3 Server Hardening 1](#_Toc85536796)

[4.8.4 Lawful Intercept requirements 1](#_Toc85536797)

[4.9 Testing 1](#_Toc85536798)

[4.9.1 Testing to be executed 1](#_Toc85536799)

[4.9.2 Tools & Test Equipment Required 1](#_Toc85536800)

[5.0 Execution section 1](#_Toc85536801)

[5.1 Timing 1](#_Toc85536802)

[5.2 Project Dependencies 1](#_Toc85536803)

[5.2.1 Project Pre-requisites 1](#_Toc85536804)

[5.2.2 Project Co-requisites 1](#_Toc85536805)

[5.2.3 Dependent or Related Projects 1](#_Toc85536806)

[5.3 Migration, Decommissioning and Redeployment Activities 1](#_Toc85536807)

[5.4 Sequencing and High Level steps 1](#_Toc85536808)

[5.4.1 Connecting to the Alcatel-Lucent 7750 SR PE router 1](#_Toc85536809)

[5.4.2 Boot option file (BOF) configurations 1](#_Toc85536810)

[5.4.3 Basic system configurations 1](#_Toc85536811)

[5.4.4 Line cards configurations 1](#_Toc85536812)

[5.4.5 Ethernet ports & Interface configurations 1](#_Toc85536813)

[**5.4.6 Logical router interfaces and router configurations** 1](#_Toc85536814)

[**5.4.7 OSPF configurations\*** 1](#_Toc85536815)

[**5.4.8 BGP configurations** 1](#_Toc85536816)

[**5.4.9 LDP configurations** 1](#_Toc85536817)

[**5.4.10 Protocol Independent Multicast (PIM) configurations** 1](#_Toc85536818)

[configuring Static Route 1](#_Toc85536819)

[**5.4.11 Service Distribution Points (SDP) configurations** 1](#_Toc85536820)

[**5.4.12 ISIS and IPv6 related prefixes and communities** 1](#_Toc85536821)

[**5.4.13 Quality of service (QoS) configurations** 1](#_Toc85536822)

[**5.4.14 Y.1731 - Network SLA Test** 1](#_Toc85536823)

[**5.4.15 System Security Configurations** 1](#_Toc85536824)

[**5.4.16 Uplink Routers – DGW Logical Interface Configuration** 1](#_Toc85536825)

[**5.4.17 Uplink Routers – DGW BGP Configuration** 1](#_Toc85536826)

[5.4.18 Uplink Routers – DGW LDP Configuration 1](#_Toc85536827)

[5.4.19 Uplink Routers – DGW Configuration 1](#_Toc85536828)

[**5.4.20 Route Reflector VPNv4 BGP Configuration** 1](#_Toc85536829)

[VPN-v4 sessions on Route reflectors (RR) and MVPN sessions on Route reflectors for AGW/DGW 1](#_Toc85536830)

[**5.4.19 DDOS configuration** 1](#_Toc85536831)

[**5.6 Regulatory Codes/Third Party Requirements** 1](#_Toc85536832)

[**5.6.1 Space and Power (as applicable)** 1](#_Toc85536833)

[**5.6.2 Fibre agreements (as applicable)** 1](#_Toc85536834)

[**5.6.3 Leased Facility agreements (as applicable)** 1](#_Toc85536835)

[**5.7 Coordination Contacts** 1](#_Toc85536836)

[**6. 0 Functional Area and Responsibility** 1](#_Toc85536837)

[**7.0 Recommended Training** 1](#_Toc85536838)

[8.0 Reference Documents 1](#_Toc85536839)

[8.1 Technology or Architecture Spec, Equipment Documentation, Standards and Guidelines 1](#_Toc85536840)

[9.0 Abbreviations and Acronyms 1](#_Toc85536841)

[Figures and Tables 1](#_Toc85536842)

# 1.0 Executive Summary

This Engineering plan describes the installation of ALU-7750 at Address PHUB.

# 2.0 Scope Section

## 2.1 Scope of Work

This Engineering Design Specification will cover installation and configuration of Alcatel- Lucent ALU-7750 router at Address.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CILI Code | Hostname | Site Address | Hardware | Type |
| CLLI |  | Address | ALU-7750 |  |

## 2.2 Benefit to the company

Provide high availability, reliable and fault torlerent services to business customers on .

## 2.3 Consequences if not done

Customer may not get connected.

## 2.4 Measurement Criteria

All new uplinks shall be turn up and carrying traffic.

## 2.5 Acceptance Summary Checklist



# 3.0 Financial Section

## 3.1 General Information

|  |  |
| --- | --- |
| **Oracle #** |  |
| **OTL #** |  |
| **RPATS/Project #:** |  |

## 3.2 Inter-company/department Charges (if applicable)

## 3.3 Bill of Materials

The following describes the equipment required for this project.

Note: Check warehouse for the equipment, if not available buy under Oracle

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RCPC Part Number** | **Vendor Part Number** | **Description** | **Currency** | **Quantity** | **Unit Price** | **Extended Price in CAD** |
|  |  |  |  |  |  |  |
| **TOTAL: CAD 0.00** | | | | | | |

## 3.4 OPEX

*N/A*

# 4.0 Technical Section

## 4.1 Solution Overview

### 4.1.1 Install at Address



Lag

Lag

### 4.1.2 Service Flow Diagram

*N/A*

## 4.2 Platform Specifications

### 4.2.1 Hardware Specifications

Please refer to Section 8, the attachment, <SR-12 Installation Guide>.

#### 4.2.1.1 Space and Power

FPE-76 already approved.

### 4.2.2 Physical Installation

#### 4.2.2.1 Card Installation

Install the following cards and transceivers on

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Slot #** | **MDA #** | **DESCRIPTION** | **Supplier Part Number** | **Note** |
|  |  |  |  |  |
| A |  | SF/CPM |  |  |
| B |  | SF/CPM |  |  |

#### 4.2.2.2 Optics Installation

Following Optics needs to be installed:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Port | Transceiver Part# | Comment | Fiber/Connector |
|  |  |  |  |  |

#### 4.2.2.3 Fiber Run

Run fiber between the following ports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A device | A Interface | Z device | Z Interface | Type |
|  |  |  |  | SMF |
|  |  |  |  | SMF |

For better identification of Uplink interfaces, a new naming convention has been established, please look for the CLFI and near shelf info in the DDP

Sample Naming convention for Uplink:

=================================================================================================================================

Description "N~ 10GE::DGW02.BLOOR:Te0/3/0/0::TOROONXNO2D-020:Shelf#1:Slot12:Port3:Ch9265 | CLFI # 5000/GE10/TOROONLQO2D/TOROONXNO2D

N~ (network interface)

10GE (speed)

:: (Divided Symbols divide the equipment)

: (one colon is to divide the components in a same equipment)

DGW02.BLOOR:Te0/3/0/0 (far end router name & interface)

TOROONXNO2D-020:Shelf#1:Slot12:Port3:Ch9265 (near end transmission equipment) (TID):shelf:slot:port:channel. This part comes from DDP.

| (decollator)

CLFI # 5000/GE10/TOROONLQO2D/TOROONXNO2D  CLFI

================================================================================================================================

### 4.2.3 Logical Network Connections

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A device** | **Lag ID** | **Port** | **Lag Interface** | **IP Address** | **Z device** | **Port** | **Z Interface** | **IP Address** |
|  | Lag | 1/1/1 | TE\_DGW\_Lag |  |  | Te0/5/0/0 | Bundle Ether |  |
| 1/1/2 |  | Te0/5/0/1 |  |
|  | 2607:F798:0010:9C17:0:721:3913:3009/64 |  | 2607:F798:0010:9C17:0:721:3913:3010/64 |
|  |  |  |  |
|  |  |  |  |
|  | Lag | 2/1/1 | TE\_DGW\_Lag |  |  | Te0/5/0/0 | Bundle Ether |  |
| 2/1/2 |  | Te0/5/0/1 |  |
|  | 2607:F798:0010:9C18:0:721:3913:3013/64 |  | 2607:F798:0010:9C18:0:721:3913:3014/64 |
|  |  |  |  |
|  |  |  |  |
|  |  |  | Loopback0 | 209.148.254.151/32 RBS -loopback-New |  |  |  |  |
|  |  |  | Loopback300 | 100.95.10.221/32 |  |  |  |  |
|  |  |  | System IP | 209.148.255.151/32  2001:0506:0020:7FC0::2091:4825:5151 |  |  |  |  |

Loopback 0 ip address of and

|  |  |  |
| --- | --- | --- |
| Hostname | Loopback 0 IPv4 address | Loopback 0 IPv6 address |
|  | 66.185.86.237/32 | 2001:506:20:7fc0:0:661:8508:6237/128 |
|  | 66.185.86.238/32 | 2001:506:20:7fc0:0:661:8508:6238/128 |

* The PHUB prefix is a /40 assigned to the PHUB that is used to assign the customer routed blocks.  It’s in the config as the “IPv6\_IGP\_BUSINESS” prefix list.
* The PHUB p2p prefix is a /60 assigned to the PHUB to use for customer p2p’s.  It’s in the config as the “IPv6\_P2P\_IGP\_ACCESS” prefix list
* The PHUB community is a community in the 812:9xxx range that is usually the same as the last four digits in the ISIS area.  It’s in the config as “<PHUBNAME>-COMM”  (ie. WLFDLE-COMM)
* The Regional community is in the config as “REGIONAL-<REGION>-COMM” (ie. REGIONAL-D-COMM)

|  |  |
| --- | --- |
| Prefix List Name | Prefix |
| IPv6\_IGP\_BUSINESS | **2606:f900:b500::/40 longer** |
| IPv6\_P2P\_IGP\_ACCESS | **2606:f900:6001:2e0::/60 longer** |

|  |  |
| --- | --- |
| Community Name | Community Member |
| **KWKW-COMM** | **812:9015** |
| **REGIONAL-C-COMM** | **812:9103** |

|  |  |
| --- | --- |
| **ISIS area-id** | **OSPF area Number** |
| area-id 03.9015 | 0.0.0.0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7750 Hostname | System IP | SDP\_ID | OSPF sub area- id | ISIS area-id |
|  | 209.148.255.151/32 | 551 | 0.0.0.0 | 03.9015 |

### 4.2.4 Network Management

The following chart specifies the console connections required for the Alcatel-lucent 7750 SR-12 Router in each location. (Manual - Chassis Installation Guide (each type has its specification), Nokia Support Portal, link )

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipment** | **Port Type Location** | **OOB Server assignment** | **OOB Line Number** |
| **Address** | | | |
| ALU 7750 SR-12  SF/CPM A | DB-9 Patch to OOB Patch | TBD | TBD |
| ALU 7750 SR-12  SF/CPM B | DB-9 Patch to OOB Patch | TBD | TBD |

Table: Console Port Requirements

Note: IPE has to run console connection to each device and assign and record the console information to IP Edge Ops

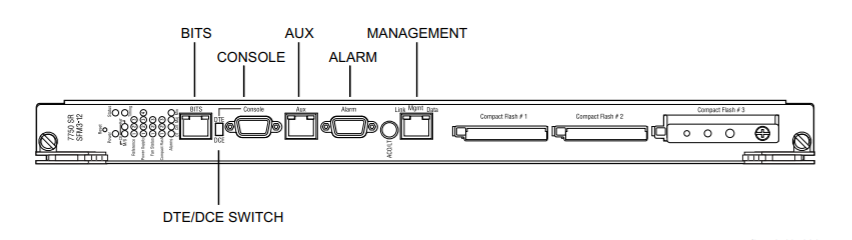


Figure : Console Port Connection

### 4.2.5 Network Timing

*N/A*

### 4.2.6 Operating System

TiMOS-C-16.0.R3-2

### 4.2.7 Initial Dimensioning

|  |  |
| --- | --- |
| **Make and Model** | **ALU-7750 -** |
| **Dimensions** |  |
| With cable management unit | 24.5 in. H x17.5 in. W x 30 in. D |
| Chassis weight (empty) | 124 lb (56.37 kg) |
| Chassis weight (loaded) | 342.5 lbs. (155.4 kg) |
| Mounting | Mount in 19-inch equipment rack.  Bracket ears are factory installed to mid-mount the  chassis in a 19-inch rack |

### 4.2.8 Application Functional Specifications

*N/A*

### 

### 4.2.9 Service Redundancy and Failover Capabilities

The design of network infrastructure and ALU-7750 Service Router can avoid single point of failure. 7750 SR-12 TiMOS supports numerous features that minimize service disruption. These features include non-stop routing, non-stop services, stateful failover, in-service software upgrades (IssUs), fast reroute, pseudowire redundancy. However, in production, not all these features are enabled.

### 

### 4.2.10 Support Services

*N/A*

### 4.2.11 Performance and Fault Management

#### 4.2.11.1 Fault Monitoring Management

*Please reference detail logical design configuration template.*

#### 4.2.11.2 Performance Monitoring Management

*Please reference detail logical design configuration template.*

### 

### 4.2.12 Compliance

*N/A*

## 

## 4.3 Configuration Details

### 4.3.1 Physical Installation of Alcatel-lucent 7750 SR12E

### Alcatel-lucent 7750 SR-12 Chassis Physical Overview



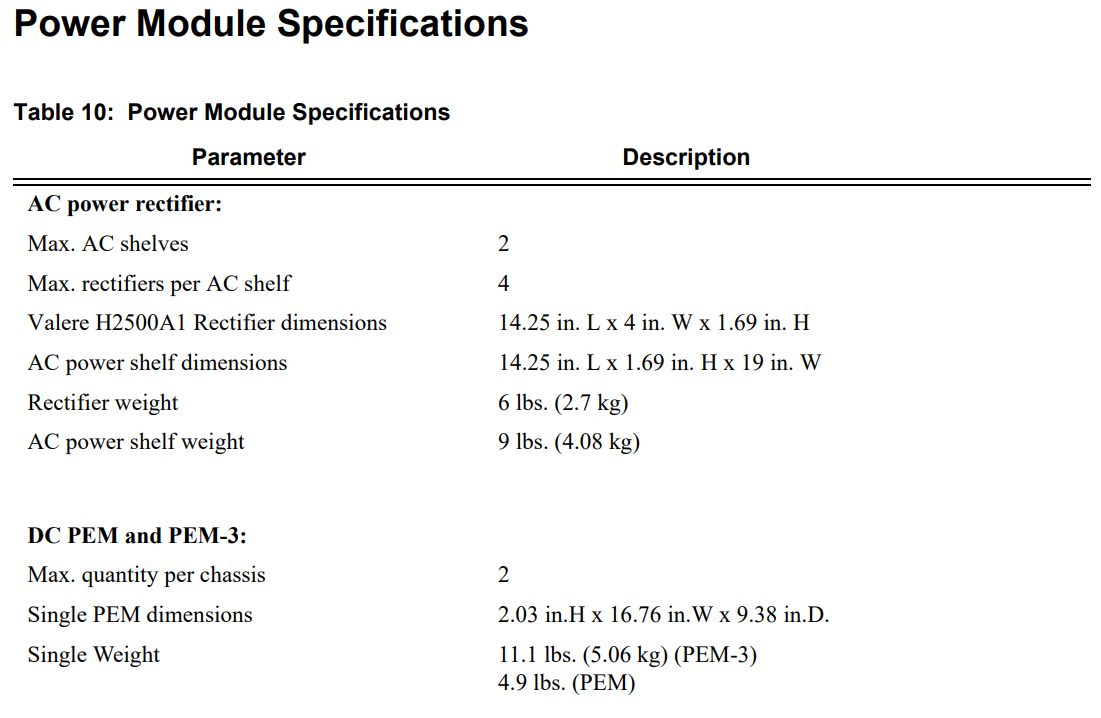


SR-12 Rear View:



****

**Power Module Specifications**

****

**Power Supplies**

Two slots in the chassis are designated for hot swappable, load-sharing, DC power entry modules

(PEMs). There are two DC PEM types: 100-Amp single-feed PEMs and 175-Amp dual-feed PEM3s.

AC power can be converted to DC power using external AC to DC rectifiers available from

Alcatel-Lucent.

**POWER REDUNDANCY**

You must install at least one DC PEM or PEM-3 in the 7750 SR-12 chassis. You can install an

additional PEM or PEM-3 for power redundancy.

If you need to convert AC power to usable DC power and you are using 100-Amp single-feed

PEMs, you can install up to two rectifiers in the same AC power shelf that you connect to your

PEM. If you need to convert AC power to usable DC power and you are using 175-Amp dual-feed

PEM-3s, you install four rectifiers in the AC power shelf that you connect to your PEM-3. For

redundant operation, you can install a second AC power shelf. Connect the second power shelf to

the second PEM or PEM-3. This ensures that the second DC PEM has an independent redundant

power source.

**DC POWER ENTRY MODULES**

You can install and remove DC PEMs from the rear of the 7750 SR-12 chassis power slots 1 and 2.

One PEM can support the full system electrical current requirements if you are operating the 7750

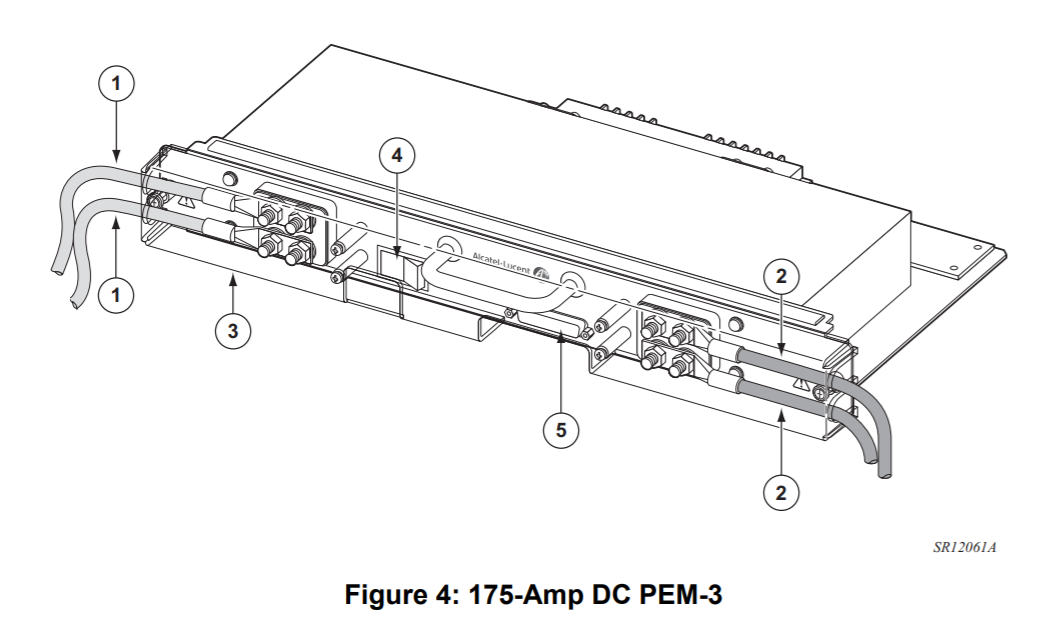
SR-12 without power redundancy. You must install two PEMs for redundancy. These PEMs must

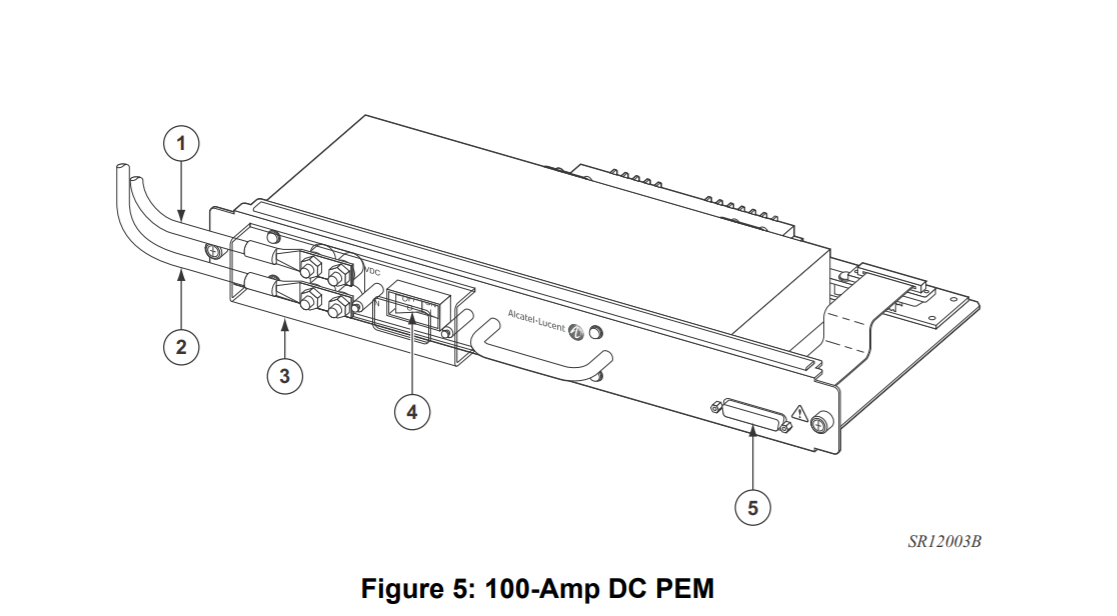
be powered on at all times. There are two types of PEMs: the 175-Amp PEM-3 and the 100-Amp

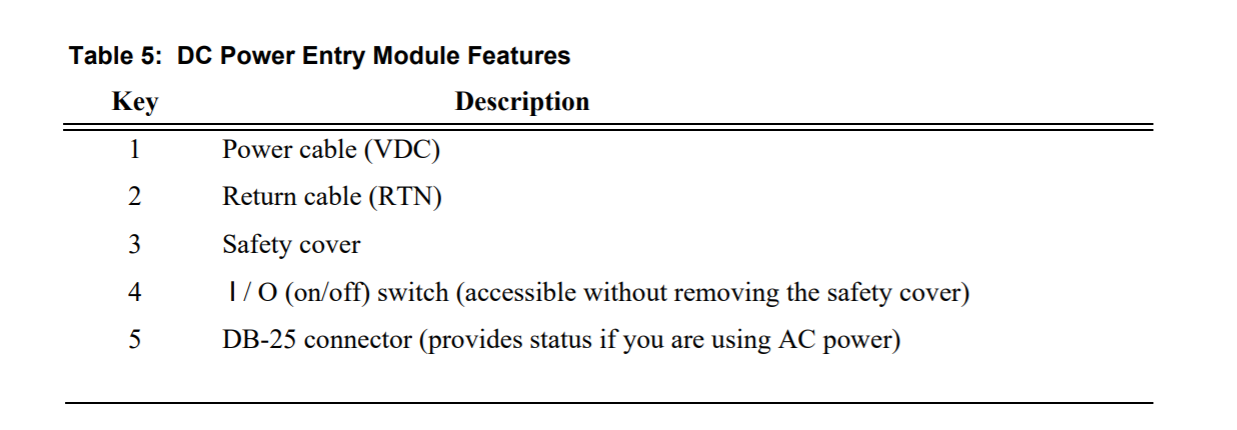
PEM. The PEM-3 is required for the 7750 SR-12 chassis when the router has one or more IOM3-

XPs, IOM3-XP-Bs, or IMMs installed. Due to increased power requirements, a 175 AMP DC

PEM-3 provides dual feeds.







**AC TO DC RECTIFIERS**

AC to DC rectifiers change 200/240V AC power to -48 VDC power.

Each power shelf can accommodate up to four 2500W AC to DC rectifiers that plug into a

common power backplane in the AC-input power shelf. You must connect each AC power shelf to

a separate PEM installed in the 7750 SR-12 chassis. For redundancy, you must install two PEMs,

each connected to a separate AC to DC rectifier shelf. You must install four rectifiers in each shelf.

The AC to DC rectifiers in each power shelf provide automatic load-sharing. When a rectifier is

removed, the remaining rectifiers adjust to fulfill the power requirements and maintain

uninterrupted system power.

The rectifiers in the AC power shelf are hot-swappable. You can remove or replace a power

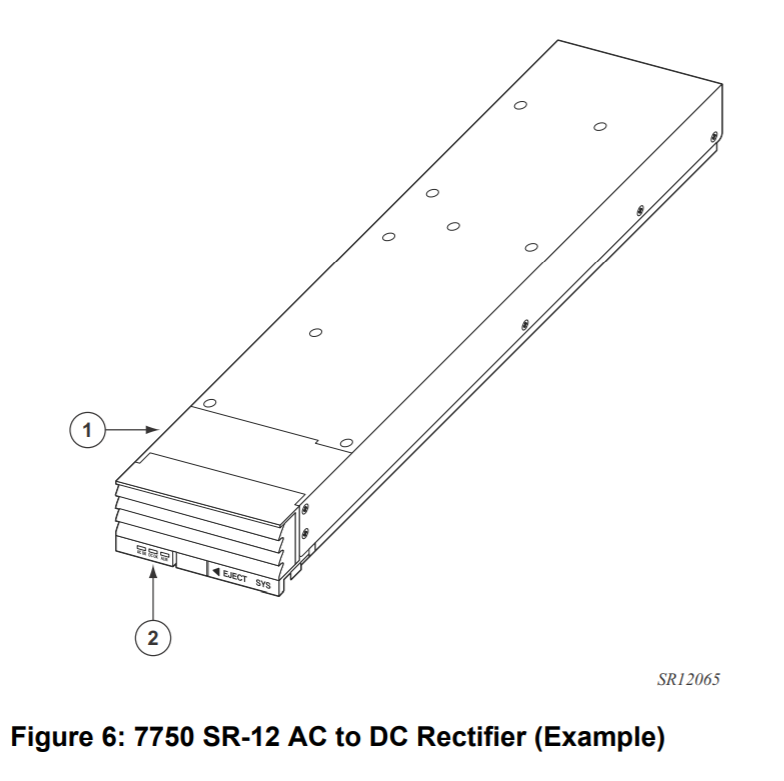
module while the system is operating without affecting system operation. For maximum

redundancy, connect each AC-input power module to a separate AC power source. The power

source (outlet) should be located near the equipment rack and be easily accessible.

The power cord serves as a disconnect device for each rectifier. To remove power to an individual

rectifier, the unit must be disconnected from the connectors.



|  |  |
| --- | --- |
| **Key** | **Description** |
| 1. | Power supply handle (Shown in black) |
| 2. | Power supply LEDs |

### 4.3.2 Alcatel-lucent ALU-7750 Hardware Layout

Install IMM cards and SFPs as per below chart

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Slot #** | **MDA #** | **DESCRIPTION** | **Supplier Part Number** | **Note** |
|  |  |  |  |  |
| A |  | SF/CPM |  |  |
| B |  | SF/CPM |  |  |

## 4.4 End to End Impact Assessment

### 4.4.1 Impact Classification

|  |  |
| --- | --- |
| **Service Impact (None, Degraded, Outage)\*:** | **None** |
| **Network Impact (None, Degraded, Threatened, Outage)\*:** | **None** |
| **Customer Impact (Small, Medium, Large, Extensive)\*:** | **None** |
| **Project Complexity (Low, Medium, High)** | **Medium** |

Note: \* - See “Service Management Process Policy” for the definitions of Service, Network and Customer Impact.

|  |  |  |
| --- | --- | --- |
| Project Complexity Assessment | Low | Involves/impacts single platform and/or network and Impact is well understood and known and/or  Unexpected outcome of changes cannot result in a customer impacting outage. |
| Medium | Impacts multiple platforms and/or networks and/or Potential for implementation failure exists.  Unexpected outcome of changes may result in service degradation or minor service outage. |
| High | Involves changes on and impacts multiple platforms or networks and/or High potential for implementation failure exists.  Unexpected outcome of changes may result in a major, severe or critical service outage. |

### 4.4.2 Impacted Network Elements and Services and Locations

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | **Potential Maintenance Windows Required** | | | | | | | | | | | |
| **REGION/Site/**  **Network Element** | | **Impacted Services** | **Jan** | **Feb** | **Mar** | **Apr** | **May** | **Jun** | **Jul** | **Aug** | **Sep** | **Oct** | **Nov** | **Dec** | |
|  | | **0** |  |  |  |  |  |  |  | **1** |  |  |  |  | |
|  | | **0** |  |  |  |  |  |  |  | **1** |  |  |  |  | |
|  | | **0** |  |  |  |  |  |  |  | **1** |  |  |  |  | |
|  | |  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  | |  |  |  |  |  |  |  |  |  |  |  |  |  | |

|  |  |
| --- | --- |
| **Total Potential Maintenance Windows Required** (should be the sum of the above) | **3** |

### 4.4.3 Partial/Complete Quarantine on Network Elements/Region

*N/A*

### 4.4.4 Teams Involved in the change implementation

IP Core Operation and EMTAC, Headend Engineer

### 4.4.5 Changes to the existing IP and Service Flows

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

### 4.4.6 Detailed Impact Assessment

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

## 4.5 Technical Pre-requisites

## 

## 4.6 Technical Co-requisites

## 4.7 Potential CBU Impacts/Risks

## 4.8 IP Flow -- Security

*N/A*

### 4.8.1 Network Security

*Please reference detail logical design configuration template.*

### 

### 4.8.2 System Classifications

### 4.8.3 Server Hardening

*Please reference detail logical design configuration template.*

### 

### 4.8.4 Lawful Intercept requirements

## 4.9 Testing

### 4.9.1 Testing to be executed

*Please reference detail logical design configuration template.*

### 

### 4.9.2 Tools & Test Equipment Required

*Please reference detail logical design configuration template.*

# 5.0 Execution section

## 5.1 Timing

|  |  |
| --- | --- |
| **Customer Requested Due Date** | NA |
| **Anticipated Completion Date** |  |

## 5.2 Project Dependencies

### 5.2.1 Project Pre-requisites

### 5.2.2 Project Co-requisites

### 

### 5.2.3 Dependent or Related Projects

## 5.3 Migration, Decommissioning and Redeployment Activities

## 5.4 Sequencing and High Level steps

Once all hardware modules are installed and the chassis is powered at site, the initial logical configuration will need to be performed through command line interface (CLI) via an out-of-band connection.

Following is the step-by-step summary of procedure:

**Stage - I: Does not require maintenance Window**

Step 1: Connect to the Alcatel-Lucent 7750 SR PE router

Step 2: Configure the boot option file (BOF)

Step 3: Perform the basic system configurations

Step 4 Configure the Line cards

Step 5 Configure the ports

Step 6 Configure the Logical router interfaces and router configurations

Step 7 Configure the System Security Configurations

Step 8: Configure OSPF/ISIS

Step 9: Configure BGP

Step 10: Configure LDP

Step 11: Configure Protocol Independent Multicast (PIM)

Step 12: Configure Service Distribution Points (SDP)

Step 13: Configure the Network Quality of service (QoS)

Step 14: Final Configuration tasks

Step 15: Configure RDI related pre-defined configurations

Step 16: Configure EPL/EVPL related pre-defined configurations

Step 17: Configure NNI related pre-defined configurations

**Stage - II: Does require a separate maintenance Window**

Step 1: Configuring the DGWs

Step 2: Configuring the route reflectors

**NOTE: Step 12 SDP configurations can be done through SAM, the configuration in this Network Integration document is for reference purpose only. SDP needs to be configured between all existing AGW’s, and new AGW/DGW’s.**

**NOTE: All configurations in the following sections are for EXAMPLE only; DO NOT CUT AND PASTE.**

### 5.4.1 Connecting to the Alcatel-Lucent 7750 SR PE router

The 7750 SR router’s console speed (baud rate) is initially configured to 115200 bit/sec by default, whereas the Rogers production terminal server line speed is 9600 bit/sec. In order to have access to the 7750 router through its console port, the baud rate of the particular line on the production terminal server to which the 7750 is connected needs to be changed to 115200.

The commands below change the line speed (baud rate) of the terminal server to 115200.

**Terminal server**

Configure terminal

Line <Line\_Number> <- The line to which the 7750 is connected

Speed 115200

Logout from the terminal server (Make sure the configuration is saved) and then connect to the 7750 PE by using reverse telnet via out-of-band connection.

[xxx@ipops xxx]$ *telnet <Production\_Terminal\_server\_IP> <Line\_number>*

Trying x.x.x.x...

Connected to x.x.x.x.

Escape character is '^]'.

User Access Verification

Username: *xxx* <- Console server authentication,enter Production TACACS+ username

Password: <- enter your TACACS+ password

Login: *admin* <- 7750 authentication, default username is admin

Password: <- default password is admin

A:NS071350914#

#### Upgrade 7750 SR OS image and the firmware on SF/CPM and IOS cards

The 7750 SR OS - TiMOS software ordered from the vendor is X.0X, the software needs to be upgraded to the version 16.0.

### 5.4.2 Boot option file (BOF) configurations

The Boot Option File (BOF) is the file that contains the parameters which specify the location of the image file that the router will try to boot from and the configuration file. It also contains the Switch Fabric/Control Processor Module (SF/CPM) console port and management port configurations.

Connect to the 7750 PE via the OOB connection to the router’s console port and configure the BOF using the command template provided below:

[xxx@ipops xxx]$ *telnet <Production\_Terminal\_server\_IP> <Line\_number>*

Trying x.x.x.x...

Connected to x.x.x.x.

Escape character is '^]'.

User Access Verification

Username: *xxx* <- console server authentication, use your tacacs+ username

Password: <- console server authentication, use your tacacs+ password

Login: *admin* <- 7750 authentication, default username is admin

Password: <- default password is admin

A:NS071350914#*admin <- enter “admin”*

A:NS071350914>admin# *save cf3:\<HOST\_Name>.cfg* **🡨 Create config file first**

A:NS071350914>admin# *exit*

A:NS071350914# *bof <- enter “bof” to configure the Boot Option file*

A:NS071350914>bof#*primary-image cf3:\7750-TiMOS-X.0.RX\*

A:NS071350914>bof#*primary-config cf3:\<HOST\_Name>.cfg*

A:NS071350914>bof#*wait 3*

A:NS071350914>bof#*persist on*

A:NS071350914>bof#*console-speed 115200*

A:NS071350914>bof#*save*

Writing BOF to cf3:/bof.cfg

Saving BOF .... Completed.

Syncing .... Completed.

The completed BOF should look like below:

A:NS071350914>bof#*show bof*

============================================================================

BOF (Memory)

============================================================================

primary-image cf3:\7750-TiMOS-X.0.RX\

primary-config cf3:\<HOST\_Name>.cfg

autonegotiate

duplex full

speed 100

wait 3

persist on

no li-local-save

no li-separate

console-speed 115200

============================================================================

### 5.4.3 Basic system configurations

The basic system configuration includes the configuration of router name, login control, system time, snmp packet size and system redundancy commands.

The redundancy command sets the redundancy option between the active and standby SF/CPM. For initial installation and any upgrade, the redundancy synchronize option should be set to ‘boot-env’. For normal operations, redundancy should be set to ‘config’.

The synchronization occurs when the admin save or bof save commands are executed. When the boot-env parameter of the synchronize command is specified, the BOF, boot.ldr, config, and image files are automatically synchronized. When the config parameter is specified, only the configuration files are automatically synchronized.

To execute synchronization manually, the admin>redundancy> synchronization command must be entered with the boot-env parameter or the config parameter. When the boot-env parameter is specified, the BOF, boot.ldr, config, and image files are synchronized. When the config parameter is specified, only the config files are synchronized.

Use the configuration template below with the parameters in the following table(s) to create the actual basic system configuration for all locations including AGW & DGW.

The configuration is same as existing in Generic Provisioning eMOP template with following differences –

* Need to configure the “chassis-mode d” as SR-7 & SR-12 chassis
* Card configuration is for IMM cards used

exit all

configure

#--------------------------------------------------

echo "System Configuration"

#--------------------------------------------------

system

name ""

#

# Chassis mode changed to ***d*** correspond to IOM3-XP cards

# Default chassis mode is ***a***

# Chassis mode is ONLY for SR7/12, NOT Applicable to SR c12

#

chassis-mode d

# Rest of configuration is same as existing

snmp

packet-size 9216

no shutdown

exit

login-control

telnet

inbound-max-sessions 7

outbound-max-sessions 7

exit

idle-timeout 30

pre-login-message "\n\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\n\nRogers Cable Inc.\nBy using this system, you agree to comply with RCI corporate policies governing accessing and using the company's IT systems and data. To protect this system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and are subject to audit. Unauthorized access or use of this system is prohibited and could be subject to disciplinary actions as well criminal and/or civil penalties.\n\n\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\n\n"

exponential-backoff

exit

time

ntp

server 24.153.22.24

server 24.153.22.152

no shutdown

exit

zone UTC

exit

exit

#--------------------------------------------------

echo "Redundancy Configuration"

#--------------------------------------------------

redundancy

synchronize boot-env

exit

exit all

admin save

Note:

Upon completion of the initial configuration, and an “admin save” command is executed, the redundancy synchronize option needs to be changed to “config’.

### 

### 5.4.4 Line cards configurations

Interface line cards include Integrated Media Modules (IMMs) 12 port 10Gig to be installed in slots 1 and 2 and IMM 48 port GE to be installed in slot 9.

IMMs can be preconfigured prior to the component installation or configured after the components are installed. Each specific slot must specify an IMM. You cannot configure ports until the MDA is configured.

Please refer to section 4.3.2 for card type and slot # .

.

Slot X is determined in section 4.2.2

#IMM 12 port 10G card will be at slotX and X.

card x

card-type imm-2pac-fp3

mda 1

mda-type p6-10g-sfp

network

ingress

pool

resv-cbs 47

slope-policy "RNS\_slope-policy"

exit

queue-policy "RNS\_network-queue"

exit

exit

no shutdown

exit

mda 2

mda-type p6-10g-sfp

network

ingress

pool

resv-cbs 47

slope-policy "RNS\_slope-policy"

exit

queue-policy "RNS\_network-queue"

exit

exit

no shutdown

exit

no shutdown

exit

# IMM 48 port card will be at slot X

card Z

card-type imm48-1gb-sfp

mda 1

network

ingress

pool

resv-cbs 47

slope-policy "RNS\_slope-policy"

exit

queue-policy "RNS\_network-queue"

exit

exit

no shutdown

exit

mda 2

network

ingress

pool

resv-cbs 47

slope-policy "RNS\_slope-policy"

exit

queue-policy "RNS\_network-queue"

exit

exit

no shutdown

exit

no shutdown

exit

exit all

# The mode of physical ports need to be manually

# changed to "access". Use the following range commands to specify the

# mode of a range of Ethernet ports to be "access"

Example:

configure port Y/1/[1..24] ethernet mode access

configure port Y/2/[1..24] ethernet mode access

Verification: making sure all the above commands have been properly entered.

Use the below commands show the card, mda and ports

- show card

- show card state

- show mda

- show system information

### 5.4.5 Ethernet ports & Interface configurations

A network port is network facing and participates in the service provider transport or infrastructure network processes.

The mode of the Ethernet ports is “network” by default, for the customer facing ports, the port mode need to be manually changed to “access”, such that the Service Awareness Management server (5620 SAM) will be able to demonstrate all access mode ports from its GUI and ready for customer provisioning.

The infrastructure part of configuration templates for AGW in a Metro extension environment should be similar as a regular AGW on RCBIN. This section only focuses on the specific configuration related to Metro extension. Use the configuration template below with the parameters for AGWs.

|  |
| --- |
| exit all  configure  #  # Following are Network facing ports (AGW) in use  # Port 1/1/1, 1/1/2, 2/1/1, 2/1/2  exit all  configure  #--------------------------------------------------  echo "Port Configuration"  #--------------------------------------------------  port X/Y/Z  description <standard port - AGW description>  network  egress  pool  resv-cbs 47  slope-policy "RNS\_slope-policy"  exit  exit  exit  ethernet  mtu 4484  network  queue-policy "RNS\_network-queue"  exit  exit  no shutdown  exit  exit all |

Use the below commands show ports:

- show port

- show system information

**5.4.6 Logical router interfaces and router configurations**

In order to provision services on a 7750 SR-Series router, logical IP routing interfaces must be configured to associate attributes such as an IP address and physical port. The logical interface will be assigned a NAME that is subsequently referenced by other processes (for example, OSPF, BGP etc).

The interface name can be up to 32 characters, but must start with a letter.

Loopback0 & System IP configuration for AGW & DGW remains same as on existing AGW’s.

Note – Please refer to Table in section 4.2.3 for Interface name facing AGW – AGW, AGW – vDGW. Following naming convention is followed –

AGW (10 Gig port) FACING AGW (10 Gig port)

TE\_VLAN90\_AGW ----VLAN 90 in OSPF area 0

TE\_VLAN91\_AGW --- VLAN 91 in OSPF area XX for all regions

AGW (10 Gig port) FACING DGW (10 Gig port)

TE\_DGW\_Lag95

TE\_DGW\_Lag96

AGW (10 Gig port) FACING vDGW (10 Gig port)

TE\_vDGW\_Lag95

AGW (10 Gig port) FACING DGW (10 Gig port)

TEx/y/z\_DGW

(Replace TE with GE if 1Gig port)

AGW ( Multiple 10GE ) Facing DGW:

TE\_DGW\_LagXX

DGW ( Multiple 10GE ) Facing DGW/AGW:

TE\_DGW\_LagXX

TE\_AGW\_LagXX

|  |
| --- |
| exit all  configure  router  lag  description "XXXXXXXXX "  port 1/1/1  port 1/1/2  dynamic-cost  lacp passive  no shutdown  exit  lag  description "XXXXXXXXXXX "  port 2/1/1  port 2/1/2  dynamic-cost  lacp passive  no shutdown  exit  **# Refer to section 4.2.3 for IPv4 & IPv6 addresses**  interface "lo0"  address XXXX  loopback  exit  interface "system"  address XXXX  ipv6  address XXXXX  exit  exit  interface "lo300"  address XXXXX  description "Ddos clean-vrf next hop"  loopback  no shutdown  exit  exit  interface "TE\_DGW\_Lag"  address XXXXX  port lag- XXXXX  ipv6  address XXXXX  exit  qos 2  cflowd interface  exit  interface " TE\_DGW\_Lag"  address XXXXX  port XXXXX  ipv6  address XXXXX  exit  qos 2  cflowd interface  exit  exit all |

Verification: making sure all the above commands have been properly entered.

Use the below commands show router interface:

- show router interface

**5.4.7 OSPF configurations\***

The new multi OSPF area design has been introduced to facilitate traffic localization and limit OSPF LSA propagation over the network. Here is a summary of the new OSPF area design:

A non-backbone OSPF area has been designated for each region, and two AGWs at each region will be the ABR (Area Board Router).

The inter-AGW link will have two logical interfaces which establish OSPF adjacency for both backbone and non-backbone area

The OSPF metrics on vDGW in Central Area are same as regular DGW (2000 for uplinks to CGW, 2500 for south bound towards AGW and 5 for inter-DGW link)

The OSPF metrics on vDGW in Both West and CENTRAL Area are different than it in Central Area (2000 for uplinks to CGW, 10 for inter-DGW link , 2500/2505 for south bound towards AGW: use different cost to avoid bigger latency link caused by physical distance)

AGW is still using same metric (2500) for its uplink to DGW. AGW uplinks to vDGWs should be same as vDGW to AGWs. The inter-AGW links has two metrics, one for backbone area is 3 and non-backbone area metric is 3000.

DGW sets 3000 for all network interfaces

MD5 authentication should be applied to all OSPF sessions

|  |
| --- |
| configure  router  #--------------------------------------------------  echo "OSPFv2 Configuration"  #--------------------------------------------------  ospf  router-id x.x.x.x  timers  spf-wait 1000 50 200  lsa-generate 5000 10 50  lsa-arrival 50  exit  graceful-restart  exit  #  # OSPF Area for is 0  #  area 0.0.0.0  interface "system"  metric 1  exit  interface "lo0"  metric 1  exit  interface "lo300"  metric 1  no shutdown  exit  #  interface TE\_DGW\_Lag XXX  interface-type point-to-point  mtu 4470  metric 2500  authentication-type message-digest  message-digest-key 1 md5 "OSPF\_Plain\_Text\_Key"  exit  interface TE\_DGW\_Lag XXX  interface-type point-to-point  mtu 4470  metric 2500  authentication-type message-digest  message-digest-key 1 md5 "OSPF\_Plain\_Text\_Key"  exit  exit  exit al |

Verification: making sure all the above commands have been properly entered.

Use the below commands show ospf status:

- show router ospf interface

- show router ospf neighbor

- show router ospf area

**5.4.8 BGP configurations**

The BGP design of this new virtual PHUB follows same policy as regular PHUB. vDGW will be the IPv4 and IPv6 route reflector for the virtual PHUB. Then it will peer with dedicated route reflector for both IPv4 and IPv6. For VPNv4, all AGWs and DGWs will have iBGP session directly with VPNv4 route reflector.

AGW - No additional BGP configuration is required on AGW for Metro extension design. AGW will have iBGP peering with vDGW50.YM & vDGW50.MTMC for IPv4/v6 routes and RR’s for VPNv4 routes.

DGW - The BGP configuration on DGW is exactly same as all AGW. DGW will have iBGP peering with vDGW50.mtnk & vDGW50.wlfdle for IPv4/v6 routes and RR’s for VPNv4 routes.

REVISION: Updated RR name for bloor and mtnk and move “RR-MVPN” group peering to bloor and mtnk.

exit all

configure

router

#--------------------------------------------------

echo "Policy Configuration"

#--------------------------------------------------

policy-options

begin

policy-statement "redistribute all"

exit

commit

exit

#--------------------------------------------------

echo "BGP Configuration"

#--------------------------------------------------

bgp

family ipv4 vpn-ipv4 ipv6 vpn-ipv6

authentication-key "<Password>" hash2

min-route-advertisement 2

local-as 812

router-id “loopback 0 address”

group "RR"

family vpn-ipv4

next-hop-self

vpn-apply-export

export "redistribute all"

graceful-restart

stale-routes-time 360

exit

peer-as 812

neighbor 66.185.86.3 <--------LO0 of vpnrr01.bloor

authentication-key "<Password>" hash2

exit

neighbor 66.185.86.4 <--------LO0 of vpnrr01.mtnk

authentication-key "<Password>" hash2

exit

exit

group "DGW"

next-hop-self

vpn-apply-export

export "redistribute all"

graceful-restart

stale-routes-time 360

exit

peer-as 812

neighbor x.x.x.x <--------LO0 of

authentication-key "<Password>" hash2

exit

neighbor x.x.x.x <--------LO0 of

authentication-key "<Password>" hash2

exit

exit

group "IPv6-RR"

description "Upstream IPv6 Peer"

family ipv6

next-hop-self

type internal

export "REDISTRIBUTE\_IPv6\_ALL" "ADD\_PHUB\_TAG" "ACCEPT"

neighbor x:x:x:x:x:x:x:x <--------LO0 of

description " BGP Peer to "

authentication-key "<Password>" hash2

exit

neighbor x:x:x:x:x:x:x:x <--------LO0 of

description " BGP Peer "

authentication-key "<Password>" hash2

exit

exit

group "static-BGP"

family ipv4

exit

group "dynamic-BGP"

family ipv4

exit

exit

group "RR-MVPN"

shutdown

family vpn-ipv4 mvpn-ipv4

next-hop-self

vpn-apply-export

export "redistribute all"

graceful-restart

stale-routes-time 360

exit

peer-as 812

neighbor 66.185.86.3 <--------LO0 of vpnrr01.bloor

authentication-key "<Password>" hash2

exit

neighbor 66.185.86.4 <--------LO0 of vpnrr01.mtnk

authentication-key "<Password>" hash2

exit

exit all

admin save

Note: Please set the next hop correctly at policy “redistribute all”. The next hop address shall be the “system” IP.

**5.4.9 LDP configurations**

Same as DGW and AGW at regular PHUB, vDGW and AGW establish LDP adjacency / session with direct connected peers. The DGW will setup LDP adjacency with direct connected AGW and/or DGW as follow. In addition, the LDP adjacency should be established on inter-AGW link for both OSPF area 0 and area X (non-area 0).

Please refer to section 4.2.3 for interface details.

|  |  |
| --- | --- |
| exit all  configure  router  #--------------------------------------------------  echo "LDP Configuration"  #--------------------------------------------------  ldp  export "export-ldp"  graceful-restart  maximum-recovery-time 360  neighbor-liveness-time 300  exit  peer x.x.x.x <--------LO0 of  exit  peer x.x.x.x <--------LO0 of  exit  exit  tcp-session-parameters  peer-transport x.x.x.x <--------LO0 of authentication-key "PS4C1u1YeqC49R/yzo3jhV07rYQP9t5h7Nsyg345YrE" hash2  exit  peer-transport x.x.x.x <--------LO0 of  authentication-key "PS4C1u1YeqD1ZVjwMbMGl9j8CRd.55d6zxiXz6qNa82" hash2  exit  interface “ TE\_DGW\_Lag” dual-stack  ipv4  no shutdown  exit  no shutdown  exit  exit  targeted-session  exit  no shutdown  exit  exit  interface “ TE\_DGW\_Lag” dual-stack  ipv4  no shutdown  exit  no shutdown  exit  exit  targeted-session  exit  no shutdown  exit  exit  #--------------------------------------------------  echo "Policy Configuration"  #--------------------------------------------------    configure  router  policy-options  begin  prefix-list ”LDP-NEIGHBORS-ALL”  prefix 24.153.0.0/24 longer  prefix 24.153.1.0/24 longer  prefix 64.71.245.0/24 longer  prefix 64.71.253.0/24 longer  prefix 66.185.86.0/24 longer  prefix 66.185.94.0/24 longer  prefix 69.63.242.0/24 longer  prefix 69.63.244.0/24 longer  prefix 69.63.245.0/24 longer  prefix 69.63.246.0/24 longer  prefix 69.63.247.0/24 longer  prefix 209.148.254.0/24 longer  prefix 209.148.255.0/24 longer  exit  prefix-list "LDP-PREFIXES-LB100"  prefix 24.153.1.0/24 longer  prefix 64.71.245.0/24 longer  prefix 64.71.253.0/24 longer  prefix 69.63.245.0/24 longer  prefix 69.63.247.0/24 longer  prefix 209.148.255.0/24 longer  exit all  # **CPM-Filter of be updated accordingly**   |  | | --- | | #--------------------------------------------------  echo "System Security Cpm Hw Filters and PKI Configuration"  #--------------------------------------------------  system  security  cpm-filter  default-action drop  ip-filter  entry 10 create  action accept  description "CPM and Flash internal communication"  match  src-ip 127.0.0.0/8  exit  exit  entry 20 create  action accept  description "SSH destination#1"  match protocol tcp  dst-port 22 65535  src-ip 66.185.80.0/20  exit  exit  entry 21 create  action accept  description "SSH destination#2"  match protocol tcp  dst-port 22 65535  src-ip 64.71.240.0/20  exit  exit  entry 22 create  action accept  description "SSH destination#3"  match protocol tcp  dst-port 22 65535  src-ip 24.153.0.0/19  exit  exit  entry 23 create  action accept  description "SSH destination#4"  match protocol tcp  dst-port 22 65535  src-ip 69.63.240.0/20  exit  exit  entry 24 create  action accept  description "SSH destination#5"  match protocol tcp  dst-port 22 65535  src-ip 69.63.252.0/22  exit  exit  entry 25 create  action accept  description "SSH destination#6"  match protocol tcp  dst-port 22 65535  src-ip 67.231.216.0/21  exit  exit  entry 30 create  action accept  description "protocol BGP"  match protocol tcp  dst-port 179 65535  exit  exit  entry 31 create  action accept  description "protocol BGP"  match protocol tcp  src-port 179 65535  exit  exit  entry 35 create  action accept  description "RIP Routing for PE-CE"  match protocol udp  dst-port 520 65535  exit  exit  entry 40 create  action accept  description "Domain DNS server using udp"  match protocol udp  dst-port 53 65535  exit  exit  entry 41 create  action accept  description "Domain DNS server using tcp"  match protocol tcp  dst-port 53 65535  exit  exit  entry 50 create  action accept  description "ftp control #1"  match protocol tcp  src-ip 66.185.80.0/20  src-port 21 65535  exit  exit  entry 51 create  action accept  description "ftp data #1"  match protocol tcp  src-ip 66.185.80.0/20  src-port 20 65535  exit  exit  entry 52 create  action accept  description "ftp control #2"  match protocol tcp  src-ip 64.71.240.0/20  src-port 21 65535  exit  exit  entry 53 create  action accept  description "ftp data#2"  match protocol tcp  src-ip 64.71.240.0/20  src-port 20 65535  exit  exit  entry 60 create  action accept  description " ICMP echo-request"  match protocol icmp  icmp-type echo-request  exit  exit  entry 61 create  action accept  description " ICMP echo-reply"  match protocol icmp  icmp-type echo-reply  exit  exit  entry 62 create  action accept  description " ICMP time-exceeded"  match protocol icmp  icmp-type time-exceeded  exit  exit  entry 63 create  action accept  description "ICMP unreachable"  match protocol icmp  icmp-type dest-unreachable  exit  exit  entry 70 create  action accept  description "ospf"  match protocol ospf-igp  exit  exit  entry 80 create  action accept  description "MCAST stream from address 224.0.0.0/24"  match protocol udp  src-ip 224.0.0.0/24  exit  exit  entry 90 create  action accept  description "NTP server#1"  match protocol udp  dst-port 123 65535  src-ip 24.153.22.24/32  exit  exit  entry 91 create  action accept  description "NTP server#2"  match protocol udp  dst-port 123 65535  src-ip 24.153.22.152/32  exit  exit  entry 100 create  action accept  description "PIM"  match protocol pim  exit  exit  entry 120 create  action accept  description "TACACS server #1"  match protocol tcp  src-ip 66.185.87.91/32  src-port 49 65535  exit  exit  entry 121 create  action accept  description "TACACS server #2"  match protocol tcp  src-ip 66.185.88.24/32  src-port 49 65535  exit  exit  entry 130 create  action accept  description "RSVP"  match protocol rsvp  exit  exit  entry 140 create  action accept  description "udp range for traceroute - optional"  match protocol udp  dst-port 32768 32768  exit  exit  entry 141 create  action accept  description "GRE Tunneling - optional"  match protocol gre  exit  exit  entry 142 create  action accept  description "vrrp - optional"  match protocol vrrp  exit  exit  entry 150 create  action accept  description "IGMP"  match protocol igmp  exit  exit  entry 200 create  action accept  description "ldp tcp/udp from Loopback0 Block1"  match  src-ip 24.153.0.0/24  exit  exit  entry 201 create  action accept  description "ldp tcp/udp from Loopback0 Block2"  match  src-ip 66.185.86.0/24  exit  exit  entry 202 create  action accept  description "ldp tcp/udp from Loopback0 Block3"  match  src-ip 66.185.94.0/24  exit  exit  entry 203 create  action accept  description "ldp tcp/udp from Loopback0 Block4"  match  src-ip 69.63.242.0/24  exit  exit  entry 204 create  action accept  description "ldp tcp/udp from Loopback0 Block5"  match  src-ip 69.63.244.0/24  exit  exit  entry 205 create  action accept  description "ldp tcp/udp from Loopback0 Block6"  match  src-ip 69.63.246.0/24  exit  exit  entry 206 create  action accept  description "ldp tcp/udp from Loopback0 Block7"  match  src-ip 209.148.254.0/24  exit  exit  entry 210 create  action accept  description "ldp tcp/udp from Loopback100 Block1"  match  src-ip 24.153.1.0/24  exit  exit  entry 211 create  action accept  description "ldp tcp/udp from Loopback100 Block2"  match  src-ip 64.71.245.0/24  exit  exit  entry 212 create  action accept  description "ldp tcp/udp from Loopback100 Block3"  match  src-ip 64.71.253.0/24  exit  exit  entry 213 create  action accept  description "ldp tcp/udp from Loopback100 Block4"  match  src-ip 69.63.245.0/24  exit  exit  entry 214 create  action accept  description "ldp tcp/udp from Loopback100 Block5"  match  src-ip 69.63.247.0/24  exit  exit  entry 215 create  action accept  description "ldp tcp/udp from Loopback100 Block6"  match  src-ip 209.148.255.0/24  exit  exit  entry 216 create  action accept  description "ldp tcp/udp from Loopback100 Block7"  match  src-ip 10.118.0.0/24  exit  exit  entry 217 create  action accept  description "ldp tcp/udp from Loopback100 Block8"  match  src-ip 10.118.30.0/24  exit  exit  entry 250 create  action accept  description "ldp tcp /udp from new P2P block1 "  match  src-ip P2P Addess (add your ipv4 address here)  exit  exit  entry 251 create  action accept  description " ldp tcp /udp from new P2P block2 "  match  src-ip P2P Address-(add your ipv4 address here)  exit  exit  entry 400 create  action accept  description "SNMP source #1"  match protocol udp  dst-port 161 65535  src-ip 66.185.80.0/20  exit  exit  entry 401 create  action accept  description "Fragmented SNMP packets - source #1"  match protocol udp  fragment true  src-ip 66.185.80.0/20  exit  exit  entry 402 create  action accept  description "SNMP source #2"  match protocol udp  dst-port 161 65535  src-ip 64.71.240.0/20  exit  exit  entry 403 create  action accept  description "Fragmented SNMP packets - source #2"  match protocol udp  fragment true  src-ip 64.71.240.0/20  exit  exit  entry 404 create  action accept  description "SNMP source #3"  match protocol udp  dst-port 161 65535  src-ip 65.97.252.149/32  exit  exit  entry 405 create  action accept  description "Fragmented SNMP packets - source #3"  match protocol udp  fragment true  src-ip 65.97.252.149/32  exit  exit  entry 406 create  action accept  description "SNMP source #4"  match protocol udp  dst-port 161 65535  src-ip 24.112.30.0/23  exit  exit  entry 407 create  action accept  description " Fragmented SNMP packets - source #4"  match protocol udp  fragment true  src-ip 24.112.30.0/23  exit  exit  entry 408 create  action accept  description "SNMP source #5"  match protocol udp  dst-port 161 65535  src-ip 24.112.32.0/23  exit  exit  entry 409 create  action accept  description " Fragmented SNMP packets - source #5"  match protocol udp  fragment true  src-ip 24.112.32.0/23  exit  exit  entry 410 create  action accept  description "SNMP source #6"  match protocol udp  dst-port 161 65535  src-ip 24.114.95.0/24  exit  exit  entry 411 create  action accept  description " Fragmented SNMP packets - source #6"  match protocol udp  fragment true  src-ip 24.114.95.0/24  exit  exit  entry 412 create  action accept  description "SNMP source #7"  match protocol udp  src-ip 24.153.0.0/24  exit  exit  entry 413 create  action accept  description " Fragmented SNMP packets - source #7"  match protocol udp  fragment true  src-ip 24.153.0.0/24  exit  exit  entry 414 create  action accept  description "SNMP source #1-Geo-Redundancy"  match protocol udp  dst-port 161 65535  src-ip 24.156.133.0/26  exit  exit  entry 415 create  action accept  description " Fragmented SNMP packets - source #1-Geo-Redundancy"  match protocol udp  fragment true  src-ip 24.156.133.0/26  exit  exit  entry 416 create  action accept  description "SNMP source #8 EBU-Arbor-TRAs"  match protocol udp  dst-port 161 65535  src-ip 192.168.227.128/27  exit  exit  entry 450 create  action accept  description "DHCP to local DHCP Server"  match protocol udp  dst-ip 255.255.255.255/32  dst-port 67 65535  src-ip 0.0.0.0/32  src-port 68 65535  exit  exit  entry 460 create  action accept  description "SSH destination#1-Geo-Redundancy"  match protocol tcp  dst-port 22 65535  src-ip 64.71.255.0/24  exit  exit  entry 461 create  action accept  description "SSH destination#2- Geo-Redundancy"  match protocol tcp  dst-port 22 65535  src-ip 66.185.87.0/24  exit  exit  entry 462 create  action accept  description "SSH destination#3-Geo-Redundancy"  match protocol tcp  dst-port 22 65535  src-ip 24.156.133.0/26  exit  exit  entry 600 create  action drop  log  match protocol \*  exit  exit  no shutdown  exit  ipv6-filter  entry 10 create  action accept  description "ALLOW telnet"  match next-header tcp  dst-port 23 65535  src-ip 2607:f798::/64  exit  exit  entry 20 create  action accept  description "ALLOW SSH"  match next-header tcp  dst-port 22 65535  src-ip 2607:f798::/64  exit  exit  entry 30 create  action accept  description "ALLOW BGP"  match next-header tcp  dst-port 179 65535  exit  exit  entry 40 create  action accept  description "Allow IPv6 ND"  match next-header ipv6-icmp  icmp-type neighbor-solicitation  exit  exit  entry 50 create  action accept  description "ALLOW IPv6 ND"  match next-header ipv6-icmp  icmp-type neighbor-advertisement  exit  exit  entry 60 create  action accept  description "Allow IPv6 ICMP"  log 101  match next-header ipv6-icmp  exit  exit  entry 70 create  action accept  description "ALLOW-SNMP"  match next-header \*  dst-port 161 65535  src-ip 2607:f798::/64  exit  exit  entry 80 create  action accept  description "ALLOW-TACACS"  match next-header tcp  src-ip 2607:f798::/64  src-port 49 65535  exit  exit  entry 90 create  action accept  description "ALLOW-DNS"  match next-header udp  dst-port 53 65535  exit  exit  entry 100 create  action accept  description "Allow NTP"  match next-header udp  dst-port 123 65535  exit  exit  entry 110 create  action accept  description "allow FTP"  match next-header tcp  dst-port 20 65535  src-ip 2607:f798::/64  exit  exit  entry 120 create  action accept  description "Allow FTP-Control"  match next-header tcp  dst-port 21 65535  src-ip 2607:f798::/64  exit  exit  entry 600 create  action drop  exit  no shutdown  exit | |

Verification: making sure all the above commands have been properly entered.

Use the below commands show LDP status:

- show router ldp interface

- show router ldp session

- show router ldp bindings

**5.4.10 Protocol Independent Multicast (PIM) configurations**

Protocol independent multicast (PIM) protocol will be used for IP multicast routing. At this point of time, only the most basic configuration needs to be implemented in the initial network integration phase as per the Technology specification.

Please refer to section 4.2.3 for interface details.

|  |
| --- |
| exit all  configure  router  #--------------------------------------------------  echo "PIM Configuration"  #--------------------------------------------------  pim  interface “TE\_DGW\_Lag”  exit  interface “ TE\_DGW\_Lag”  exit  exit  exit all |

Verification: making sure all the above commands have been properly entered.

Use the below commands show PIM status:

- show router pim interface

- show router pim neighbor

### configuring Static Route

/configure router static-route 100::/64 black-hole

/configure router static-route ::/0 next-hop DGW01-V6-P2P-ADDRESS preference 1

/configure router static-route ::/0 next-hop DGW02-V6-P2P-ADDRESS preference 255

**5.4.11 Service Distribution Points (SDP) configurations**

A service distribution point (SDP) acts as a logical way to direct traffic from one router to another through a uni-directional (one-way) service tunnel. The SDP terminates at the far-end device which directs packets to the correct service egress SAPs on that device. A distributed service consists of a configuration with at lCENTRAL one SAP on a local node, one SAP on a remote node, and an SDP binding the service to the service tunnel.

An SDP from the local device to a far-end router requires a return path SDP from the far-end SR Series back to the local router. Each device must have an SDP defined for every remote router to which it wants to provide service. SDPs must be created first, before a distributed service can be configured.

The SDPs need to be created in a fully meshed fashion on each of the 7750 PE to all other 7750 PEs, and between all AGW’s to DGW’s & DGW’s to all AGW’s & DGW’s. The SDP\_ID needs to be locally unique and approach to create SDP\_ID is mentioned below.

Note: Please follow the following guidelines when installing new ALU routers in EON Network. This applies to Network Standardization 2013 Project as well.

Historically, the SDP ID pointing to other ALU is the last octet of the far-end ALU router’s system.(e.g. if far-end ALU’s system IP is 64.71.245.101, then the SDP ID pointing to that far-end ALU on the local router is 101).

This approach is not scalable.

System IP address assigned to different ALU routers may have same last octet value since the Rogers infrastructure IP block where the ALU system IP address is allocated comprising many /24 subnet. SDP ID has to be locally unique so if two or more ALU routers’ system interface IPs has a same last byte value, the above SDP naming convention would not work since it is not able to identify two different far-ends SDP.

Thus, a new SDP naming convention is created. The SDP ID will NOT be the ALU router’s last octet value of its system IP address; rather, it will be manually assigned starting from 300 and moving onwards. Append the last 2 digits in last octet of system IP with 3 in the beginning. If the last octet has a single digit, add a 0 before it to make it 2-digit.Forexample, agw07.wlfdle has system IP of 69.63.247.9, so its SDP ID will be 309.

SDP naming convention for CMTS remains same, no changes to it.

**AGW/DGW**

exit all

configure

service

#--------------------------------------------------

echo "Service Configuration"

#--------------------------------------------------

sdp XXX mpls create

description <"SDP to xgw0x.PHUB\_Name">

far-end <far-end-ip-address>

ldp

keep-alive

shutdown

exit

no shutdown

exit

exit all

Verification: making sure all the above commands have been properly entered.

Use the below commands show SDP status:

- show service sdp

**5.4.12 ISIS and IPv6 related prefixes and communities**

According to Rogers IPv6 standard, the new vDGW’s and enclosed metro area networks will be treated as a new PHUB. Same ISIS routing policies for PHUB area apply to this new virtual PHUB.

1. The vDGW, AGW and DGW’s L1/L2-type and the adjacency between them are L1/L2
2. The Net address should following existing PHUB standard
3. Both logical interfaces created for OSPF are required for ISIS.
4. ISIS wide metric is mandatory for both level 1 and level 2
5. DGW and AGW should use same metric as other PHUB, the inter-AGW link’s metric is 3 for both L1 and L2. DGW metric to AGW and other DGW is 2000

**Please refer to section 4.2.3 for interface and area-id details.**

As a new EDS < EPS140501082 - RBS IPv6 Implementation> is issued, some prefix list and communites has to be defined. Pleae refer to this EDS and section 4.2.3 to implement necessary prefix list, communities and QoS profiles.

|  |
| --- |
| exit all  configure  router  #--------------------------------------------------  echo "ISIS Configuration"  #--------------------------------------------------  Isis  suppress-default  graceful-restart  exit  area-id xx.xxxx  lsp-lifetime 65535  no ipv4-routing  ipv6-routing mt  multi-topology  ipv6-unicast  exit  spf-wait 2 50 200  level 1  wide-metrics-only  exit  level 2  wide-metrics-only  exit  interface "system"  exit  interface “TE\_DGW\_Lag”  hello-authentication-key <isis-md5>  hello-authentication-type message-digest  interface-type point-to-point  level 1  ipv6-unicast-metric 2000  exit  level 2  ipv6-unicast-metric 2000  exit  exit  interface “TE\_DGW\_Lag”  hello-authentication-key <isis-md5>  hello-authentication-type message-digest  interface-type point-to-point  level 1  ipv6-unicast-metric 2000  exit  level 2  ipv6-unicast-metric 2000  exit  exit  exit all  Note by Sidong:  According to updated technology specification < Rogers Dedicated Internet Service Technology Specifications.docx>, the ISIS config shall be corrected. |

Verification – Making sure all the above commands have been properly entered.

Use the below commands show ISIS status:

* show router isis interface
* show router isis adjacency
* show router isis status

**5.4.13 Quality of service (QoS) configurations**

AGW & DGW will deploy same QoS policies as of existing AGW.

**5.4.14 Y.1731 - Network SLA Test**

Note: Due to hardware limitations on ALU 7750 i.e. IOM2/CFM2 cards which does not support more than 100 SDP bindings per VPLS, so we cannot bind >100 SDPs in VPLS 13 cloud (Y1731 VPLS cloud). Interim solution in agreement with Product Management is to exclude all DGW’s and keeps only one AGW per ring and per PHUB/POP site until IOM2/CFM2’s are replaced by IOM3/CFM3 or higher which will support up to 256 SDP bindings in VPLS. Also it’s been proposed to ALU to develop Service Portal (SP) feature to create Y1731 2-way test between two nodes on-demand which may take longer.

This engineering plan provides the list of AGW’s which will be part of Y1731 VPLS 13 cloud and procedure to exclude rest of nodes from Y1731 VPLS cloud. In future for any net new 7750 installed, it will not be part of Y1731 “VPLS 13” cloud unless there is no 7750 on that site and not part of metro ring.

**5.4.15 System Security Configurations**

System security configurations includes the configurations of application source-address; Authentication, Authorization and Accounting (AAA); local maintained username/password; CPM filters and queues; event logging; SNMP; SSH etc.

All system related configuration remains same except below are updates -

Updating snmp-trap-group 98, Netcool is removed from targets.

Add new accounting policies 21 & 22, changed file-id’s location to cf2:

|  |
| --- |
| exit all  configure  #--------------------------------------------------  echo "Log Configuration"  #--------------------------------------------------  log  file-id 1  location cf2:  rollover 2880 retention 168  exit  file-id 21  description "File-ID for 15 minute billing data"  location cf2:  rollover 60 retention 12  exit  file-id 22  description "File-ID for 5 minute billing data"  location cf2:  rollover 60 retention 12  exit  file-id 99  description "File-id for EoN Y1731 Network SLA"  location cf2:  rollover 60 retention 72  exit  accounting-policy 21  description "Accounting Policy for 15 minute billing data"  record combined-network-ing-egr-octets  default  to file 21  no shutdown  exit  accounting-policy 22  description "Accounting Policy for 5 minute billing data"  record complete-service-ingress-egress  default  to file 22  no shutdown  exit  accounting-policy 99  description "Accounting policy for EoN Y1731 Network SLA"  record saa  collection-interval 15  to file 99  no shutdown  exit  event-control "chassis" 2058 generate critical  event-control "chassis" 2059 generate critical  event-control "chassis" 2063 generate critical  event-control "chassis" 2129 generate critical  event-control "igmp" 2005 suppress  event-control "video" 2009 suppress  event-control "video" 2010 suppress  event-control "vrtr" 2034 generate  syslog 1  address 66.185.88.10  facility local3  no log-prefix  exit  snmp-trap-group 98  description "5620sam"  trap-target "0010E00DF99E:main1" address 24.156.133.48 snmpv3 notify-community "snmpV3User" security-level privacy  trap-target "0010E00DF99E:main2" address 24.156.133.17 snmpv3 notify-community "snmpV3User" security-level privacy  trap-target "24.156.133.17:162" address 24.156.133.17 snmpv3 notify-community "snmpV3User" security-level privacy  trap-target "24.156.133.48:162" address 24.156.133.48 snmpv3 notify-community "snmpV3User" security-level privacy  exit  log-id 90  description "System Log saved in CF2:\"  from main security change  to file 1  no shutdown  exit  log-id 91  description "System Log to Log Server"  from main security change  to syslog 1  no shutdown  exit  log-id 98  from main security change  to snmp 1024  no shutdown  exit  log-id 99  from main security change  no shutdown  exit  exit  exit all |

Verification – Making sure all the above commands have been properly entered.

Use the below commands:

* show log file-id
* show log accounting-policy
* show log snmp-trap-group
* show log snmp-trap-group 98

**5.4.16 Uplink Routers – DGW Logical Interface Configuration**

On both and add the logical interfaces to connect to .

**,**

**Refer to section 4.2.3 and above table for port details and IPv4/IPv6 address assignment for DGWs bundles and**

!Interface configuration

!

interface Bundle-Ether<bundle-id>

description **<**circuit-description**>**

mtu 4484

service-policy output POLICY\_EGRESS

service-policy input POLICY\_INGRESS

ipv4 address <P to P IPv4 address>/30

ipv6 nd suppress-ra

ipv6 address <PtoP IPv6 address>/64

ipv6 enable

 bundle minimum-active links 1

load-interval 30

flow ipv4 monitor FNF\_MONITOR\_MAP sampler FNF\_SAMPLER\_MAP ingress

!

interface TenGigE<Interface-id>

description <Interface-description>

bundle id <bundle-id> mode active

cdp

carrier-delay up 1 down 0

load-interval 30

dampening

no shutdown

**5.4.17 Uplink Routers – DGW BGP Configuration**

On both and add BGP sessions for .

**,**

!

router bgp 812

neighbor x.x.x.x ----- loopback 0

use neighbor-group AGW\_IPV4

description

!

neighbor x.x.x.x.x.x.x 🡨 AGW-SYSTEM-ADDRESS-IPv6

use neighbor-group AGW\_IPV6

description

!

!

### 5.4.18 Uplink Routers – DGW LDP Configuration

On both and add LDP sessions for .

**,**

!

mpls ldp

neighbor <AGW-ipv4-System-address> password <ldp password>

### 5.4.19 Uplink Routers – DGW Configuration

On both and add configuration interfaces connected to **to routing protocols.**

**,**

router ospf 812

area 0.0.0.0

interface Bundle-Ether<bundle-id>

cost <ospf-cost> !! use 2500

message-digest-key 1 md5 <ospf-key>

network point-to-point

mpls ldp sync

!

router isis 812

interface Bundle-Ether<bundle-id>

circuit-type level-1-2

point-to-point

hello-padding disable

hello-password hmac-md5 <isis-PWD>

address-family ipv6 unicast

metric <isis-metric> !!! use 2000

!

mpls ldp

interface Bundle-Ether<bundle-id>

!

mpls traffic-eng

interface Bundle-Ether<bundle-id>

!

multicast-routing

address-family ipv4

interface Bundle-Ether<bundle-id>

enable

!

rsvp

interface Bundle-Ether<bundle-id>

!

Attched Documents :IP-CORE Reference Guidelines – Connecting AGWs to DGW or vDGW(MPLS, RSVP, Service-Policy, LDP, PIM)



**5.4.20 Route Reflector VPNv4 BGP Configuration**

VPN-v4 sessions on Route reflectors (RR) and MVPN sessions on Route reflectors for AGW/DGW

#### Note regarding the Blue lines: These lines are required under global BGP configuration on the RR. If all address families are on same router, then those lines are not required second time to enable ‘ ipv4 mvpn address-family’ on same RR. But if VPNv4 and mdt address family are on one RRs and MPVN address family on another RR, then those line will be required on both RRs

**RR**

!

router bgp 812

neighbor “loopback 0 address” inherit peer-session IBGP

neighbor “loopback 0 address” description peer session with

address-family vpnv4

neighbor “loopback 0 address” activate

neighbor “loopback 0 address” send-community extended

neighbor “loopback 0 address” inherit peer-policy VPNV4-PE

**MVPN**

!

router bgp 812

neighbor “loopback 0 address” inherit peer-session IBGP

neighbor “loopback 0 address” description peer session with

address-family ipv4 MVPN

neighbor “loopback 0 address” activate

neighbor “loopback 0 address” send-community extended

neighbor “loopback 0 address” inherit peer-policy MVPN

**5.4.19 DDOS configuration**

|  |  |  |
| --- | --- | --- |
| Info | Purpose | Detail |
| lo300 IP address | 100.95.10.221/32 |  |
| Region(CENTRAL/CENTRAL/WEST) | CENTRAL |  |
| TRA/TMS | 192.168.227.143 (doc bellow) |  |
| Site address | Address |  |
| Site ID | Site Name |  |
| Y1731 nodal group | For Y1731 setup |  |



* Configure DDoS related configuration on AGW (Region : CENTRAL)

exit all

configure router mpls

path "to-DGW66.YM-from local node name" Check DDoS document

hop 10 remote\_CGW\_Lo0 (69.63.246.188) loose

hop 20 P-P-CSDE\_END\_IP (209.148.231.246) strict

no shutdown

exit

lsp "to-Ebu-mp01.YM- local\_node\_name"

to Remote-CSDE-Lo0 (69.63.246.30)

cspf

ldp-over-rsvp exclude

vprn-auto-bind exclude

no igp-shortcut

no bgp-shortcut

bgp-transport-tunnel exclude

primary "to-DGW66.YM-from local\_node\_name"

exit

no shutdown

exit

no shutdown

exit all

configure service

sdp 601 mpls create

description "SDP to DGW66.YM"

signaling off

far-end Remote-CSDE-Lo0 (69.63.246.30)

lsp "to-Ebu-mp01.YM -local\_node\_name"

keep-alive

shutdown

exit

no shutdown

exit

exit all

configure router policy-options

begin

community "TMS\_RT\_IMPORT\_CENTRAL \_REGION" members "target:812:8108"

community "DDoS\_CENTRAL\_REGION" members "812:807"

community "DDoS\_CENTRAL\_REGION\_PLATFORM" members "812:810"

policy-statement "IMPORT\_DEFAULT\_ROUTE"

entry 10

from

protocol bgp-vpn

community "TMS\_RT\_IMPORT\_ CENTRAL\_REGION"

exit

action accept

next-hop Remote-CSDE-Lo0 (69.63.246.30)

exit

exit

exit

policy-statement "NO\_EXPORT"

default-action reject

exit

policy-statement "AGW\_FLOWSPEC\_IMPORT"

entry 10

from

protocol bgp

community "DDoS\_CENTRAL\_REGION"

exit

action accept

exit

exit

entry 20

from

protocol bgp

community "DDoS\_CENTRAL\_REGION\_PLATFORM"

exit

action accept

exit

exit

entry 30

from

protocol bgp

community "KWKW-COMM"

exit

action accept

exit

exit

default-action next-policy

exit

exit

commit

exit all

configure service

customer 10002 create

description "DDoS-VPRN40-50"

exit

vprn 40 customer 10002 create

description "EBU-CENTRAL-Region-DDoS-DIRTY-VRF"

vrf-import "IMPORT\_DEFAULT\_ROUTE"

autonomous-system 812

route-distinguisher 812:39996

spoke-sdp 601 create

exit

no shutdown

exit all

configure router bgp

group "PEAKFLOW"

family ipv4 ipv6 flow-ipv4

neighbor TRA-Lo0-IP (192.168.227.143)

authentication-key R0T0router

import "AGW\_FLOWSPEC\_IMPORT" "ACCEPT\_IPv6\_BLACKHOLE" "ACCEPT\_BLACKHOLE"

export "NO\_EXPORT"

peer-as 812

exit

exit all

admin save

configure router policy-options

begin

community "TMS-clean-export\_CENTRAL \_REGION" members "target:812:8110"

policy-statement "TMS-clean-export\_CENTRAL\_REGION"

entry 10

action accept

community add "TMS-clean-export\_CENTRAL\_REGION"

exit

exit

exit

commit

exit all

configure service

vprn 41 customer 10002 create

info

description "TMS-clean-vrf"

vrf-export "TMS-clean-export\_CENTRAL\_REGION"

autonomous-system 812

route-distinguisher 812:39997

auto-bind-tunnel

resolution any

exit

grt-lookup

enable-grt

exit

exit

bgp

rib-management

ipv4

leak-import "VPRN41-leak-import"

exit

exit

no shutdown

exit

no shutdown

**5.5 Migration steps**

**5.6 Regulatory Codes/Third Party Requirements**

**5.6.1 Space and Power (as applicable)**

**5.6.2 Fibre agreements (as applicable)**

*<Outline what is pending resolution and who is managing the issue>*

**5.6.3 Leased Facility agreements (as applicable)**

**5.7 Coordination Contacts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Company** | **Contact Number** |
|  | **New Grad** | **Rogers Communications** | **4165205528** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**6. 0 Functional Area and Responsibility**

| 1. **Functional Area** | **Responsibility** |
| --- | --- |
| Enterprise IP Planning | Issue Engplan for configs of ALU-7750 SR-12e. |
| Equipment Engineering | Install/power/cable ALU-7750 SR12. |
| IP Planning (IP Core) | Issue/Review Engplan for Route Reflectors and DGWs and issue MOP |
| IP Core (OPS) | Configure DGW and Route Reflectors |
| Enterprise IP Ops | Confiure & test ALU-7750 SR12e |

**7.0 Recommended Training**

*N/A*

# 8.0 Reference Documents



## 8.1 Technology or Architecture Spec, Equipment Documentation, Standards and Guidelines

# 9.0 Abbreviations and Acronyms

# Figures and Tables