13-SDMS-10

REV. 00

SPECIFICATIONS

FOR

METRO ETHERNET

CONTENTS

1 Introduction

1.1 Objectives

The aim of this document is to give the specifications for a Metro Ethernet network, with carrier grade performance, supporting the requirements for the deployment of an FTTx network in Kingdom of Saudi Arabia.

1.2 Scope

This document specifies the minimum requirements for the supply, installation, configuration, testing, and commissioning of Ethernet Switches, as part of the SEC Metro Ethernet Network, covering Access and Aggregation requirements.

The primary requirements are to meet SEC's requirements for:

- Smart meter access to the GPON network via an ONT, to aggregate the multiple feeds from smart meters to an ONT located at a Meter Room, for aggregation and onward transport over the GPON network to the OLT, via the NG Provider Edge (PE) router, co-located with the OLT in an MDN station.
- An aggregation switch to provide a set of Ethernet ports to connect all services that are to be delivered to the NG PE router at an MDN station

2 Applicable codes and standards

This Distribution material standard specification shall be read in conjunction with the latest revision of Distribution General Specification titled "01-SDMS-01, Rev 01" which shall be considered as an integral part of this standard. This material standard specification shall also be read in conjunction with purchase order or contract schedules for the project, as applicable.

The latest revision/amendments of the following codes and standards shall be applicable for the equipment/material covered in this Distribution material standard specification. In case of conflict, the supplier/manufacturer may propose equipment/material conforming to one group of industry codes and standards quoted hereunder without jeopardizing the requirements of this standard specification.

- IEEE 802.1 Bridging & Management
- IEEE 802.3 Ethernet
- IEEE 1613 Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations
- IEC 61850-3 Communication Networks & Systems in Substation
- IETF RFC 768 User Datagram Protocol

- IETF RFC 791 Internet Protocol
- IETF RFC 792 Internet Control Message Protocol
- IETF RFC 793 Transmission Control Protocol
- IETF RFC 1034 Domain names - concepts and facilities
- IETF RFC 1035 Domain names - implementation and specification
- IETF RFC 1122 Requirements for Internet Hosts - Communication Layers
- IETF RFC 1321 The MD5 Message-Digest Algorithm
- IETF RFC 1661 The Point-to-Point Protocol (PPP)
- IETF RFC 1662 PPP in HDLC-like Framing
- IETF RFC 1981 Path MTU Discovery for IP version 6
- IETF RFC 1991 Path MTU discovery
- IETF RFC 1997 BGP Communities Attribute
- IETF RFC 2328 OSPF Version 2
- IETF RFC 2370 The OSPF Opaque LSA Option
- IETF RFC 2401 Security Architecture for the Internet Protocol
- IETF RFC 2402 IP Authentication Header
- IETF RFC 2406 IP Encapsulating Security Payload (ESP)
- IETF RFC 2439 BGP Route Flap Damping
- IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- IETF RFC 2461 Neighbour Discovery for IP Version 6 (IPv6)
- IETF RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- IETF RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- IETF RFC 2475 An Architecture for Differentiated Service
- IETF RFC 2508 Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
- IETF RFC 2597 Assured Forwarding PHB Group
- IETF RFC 2598 An Expedited Forwarding PHB
- IETF RFC 2675 IPv6 Jumbograms
- IETF RFC 2711 IPv6 Router Alert Option
- IETF RFC 2740 OSPF for IPv6
- IETF RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP
- IETF RFC 2858 Multiprotocol Extensions for BGP-4
- IETF RFC 2918 Route Refresh Capability for BGP-4
- IETF RFC 3031 Multiprotocol Label Switching Architecture
- IETF RFC 3032 MPLS Label Stack Encoding

- IETF RFC 3036 LDP Specification
- IETF RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option
- IETF RFC 3122 Extensions to IPv6 Neighbour Discovery for Inverse Discovery Specification
- IETF RFC 3140 Per Hop Behaviour Identification Codes
- IETF RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
- IETF RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
- IETF RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
- IETF RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
- IETF RFC 3473 Generalized Multi-Protocol Label Switching (GMPLS) Signalling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions
- IETF RFC 3477 Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)
- IETF RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
- IETF RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
- IETF RFC 3623 Graceful OSPF Restart
- IETF RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- IETF RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- IETF RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels.
- IETF RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
- IETF RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
- IETF RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- IETF RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
- IETF RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- IETF RFC 4486 Subcodes for BGP Cease Notification Message
- IETF RFC 4724 Graceful Restart Mechanism for BGP
- MEF 2 Requirements and Framework for Ethernet Service Protection
- MEF 3 Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks
- MEF 4 Metro Ethernet Network Architecture Framework Part 1: Generic Framework
- MEF 6.2 EVC Ethernet Services Definitions Phase 3 (supersedes MEF 6.1)

- MEF 7.2 Carrier Ethernet Information Model (supersedes MEF 7.1 and MEF 7.1.1)
- MEF 8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
- MEF 9 Abstract Test Suite for Ethernet Services at the UNI
- MEF 10.3 Ethernet Services Attributes Phase 3 (supersedes MEF 10, MEF 10.1, MEF 10.1.1, MEF 10.2 and MEF 10.2.1)
- MEF 10.3.1 Composite Performance Metric (CPM) Amendment to MEF 10.3
- MEF 11 User Network Interface (UNI) Requirements and Framework
- MEF 12.1 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer (supersedes MEF 12.1 and MEF 12.1.1)
- MEF 13 User Network Interface (UNI) Type 1 Implementation Agreement
- MEF 14 Abstract Test Suite for Traffic Management Phase 1
- MEF 15 Requirements for Management of Metro Ethernet Phase 1 Network Elements
- MEF 16 Ethernet Local Management Interface
- MEF 17 Service OAM Framework and Requirements
- MEF 18 Abstract Test Suite for Circuit Emulation Services
- MEF 19 Abstract Test Suite for UNI Type 1
- MEF 20 UNI Type 2 Implementation Agreement
- MEF 21 Abstract Test Suite for UNI Type 2 Part 1 Link OAM
- MEF 22.1 Mobile Backhaul Phase 2 Implementation Agreement (supersedes MEF 22)
- MEF 22.1.1 Amendment to MEF 22.1 – Small Cell Backhaul
- MEF 23.1 Class of Service Phase 2 Implementation Agreement (supersedes MEF 23)
- MEF 24 Abstract Test Suite for UNI Type 2 Part 2 E-LMI
- MEF 25 Abstract Test Suite for UNI Type 2 Part 3 Service OAM
- MEF 26.1 External Network Network Interface (ENNI)–Phase 2 (supersedes MEF 26, MEF 26.0.1, MEF 26.0.2 and MEF 26.0.3)
- MEF 27 Abstract Test Suite For UNI Type 2 Part 5: Enhanced UNI Attributes & Part 6: L2CP Handling
- MEF 28 External Network Network Interface (ENNI) Support for UNI Tunnel Access and Virtual UNI
- MEF 29 Ethernet Services Constructs
- MEF 30.1 Service OAM Fault Management Implementation Agreement Phase 2 (supersedes MEF 30)
- MEF 30.1.1 Amendment to SOAM FM IA
- MEF 31 Service OAM Fault Management Definition of Managed Objects
- MEF 32 Requirements for Service Protection Across External Interfaces

- MEF 33 Ethernet Access Services Definition
- MEF 34 ATS for Ethernet Access Services
- MEF 35 Service OAM Performance Monitoring Implementation Agreement (supersedes MEF 35)
- MEF 36.1 Service OAM SNMP MIB for Performance Monitoring (supersedes MEF 36)
- MEF 37 Abstract Test Suite for ENNI
- MEF 38 Service OAM Fault Management YANG Modules
- MEF 39 SOAM Performance Monitoring YANG Module
- MEF 40 UNI and EVC Definition of Managed Objects (SNMP)
- MEF 41 Generic Token Bucket Algorithm
- MEF 42 ENNI and OVC Definition of Managed Objects (SNMP)
- MEF 43 Virtual NID (vNID) Functionality for E-Access Services
- MEF 44 Virtual NID (vNID) Definition of Managed Objects (SNMP)
- MEF 45 Multi-CEN L2CP
- MEF 46 Latching Loopback Protocol and Functionality
- MEF 47 Carrier Ethernet Services for Cloud implementation Agreement
- MEF 48 Service Activation Testing
- MEF 49 Service Activation Testing Control Protocol and PDU Formats
- MEF 49.0.1 Amendment to Service Activation Testing Control Protocol and PDU Formats
- MEF 50 Service Operations Guidelines
- MEF 51 OVC Services Definitions

In case there are conflicts between this standard and other SEC Distribution material/engineering standards, related SEC Distribution material standards and specifications, SEC standard drawings and industry codes and standards, SEC department shall be consulted and a ruling in writing shall be obtained.

Any deviations, providing less than the minimum requirements of this standard require written approval of SEC.

3 Abbreviations

- API Application Programming Interface
- AS Autonomous System
- BFD Bidirectional Forwarding Detection
- BGP Border Gateway Protocol
- BSS Business Support System

- CBWFQ Class Based Weighted Fair Queuing
- CE Customer Edge
- CIR Committed Interface Rate
- CORBA Common Object Request Broker Architecture
- COS Class of Service
- DDOS Distributed Denial of Service
- DiffServ Differentiated Services
- DNS Domain Name System
- DSCP Differentiated Services Code Point
- DSL Digital Subscriber Line
- DVB Digital Video Broadcasting
- DWRR Deficit Weighted Round Robin
- eBGP External Border Gateway Protocol
- EGP Exterior Gateway Protocol
- EIR Exceeding Information Rate
- E-LSP EXP inferred PSC LSP
- EML Element Management Level
- EMS Element Management System
- FBB Functional Building Block
- GNE Gateway Network Element
- GSM Global System for Mobile communications
- iBGP Internal Border Gateway Protocol
- ICMP Internet Control Message Protocol
- IEC Intelligent energy controller
- IGP Interior Gateway Protocol
- INM Integrated Network Management
- IP Internet Protocol
- IPv4 Internet Protocol version 4
- IPv6 Internet Protocol version 6
- LAN Local Area Network
- LDP Label Distribution Protocol
- LSA Link State Advertisement
- LSP Label Switched Path
- MBS Maximum Burst Size
- MD5 Message-Digest algorithm 5
- MPLS Multi Protocol Label Switching

- MPLS EXP Multi Protocol Label Switching Experimental Bits
- MSTP Multiple Spanning Tree Protocol
- MTU Maximum Transmission Unit
- NE Network Element
- NHOP Next Hop
- NML Network Management Level
- NMS Network Management System
- NNHOP Next Next Hop
- NTP Network Time Protocol
- OAM Operations, Administration and Maintenance
- OSPF Open Shortest Path First
- OSS Operational Support System
- PE Provider Edge Router
- POP Point of Presence
- POS Packet over SONET
- PPP Point to Point Protocol
- PQ Priority Queue
- QoS Quality of Service
- RADIUS Remote Authentication Dial In User Service
- RED Random Early Detection
- RSTP Rapid Spanning Tree Protocol
- RSVP Resource Reservation Protocol
- RSVP-TE Resource Reservation Protocol – Traffic Engineering
- RTU Remote Terminal Unit
- SAS Substation automation system
- SDH Synchronous Digital Hierarchy
- SNMP Simple Network Management Protocol
- SONET Synchronous Optical Networking
- S/S Substation
- SSH Secure Shell
- STM Synchronous Transport Module
- STP Spanning Tree Protocol
- TACACS Terminal Access Controller Access-Control System
- TE Traffic Engineering
- TE-LSP Traffic Engineering - Label Switched Path
- TCP Transmission Control Protocol

- TDM Time Division Multiplexing
- TFTP Trivial File Transfer Protocol
- TMN Telecommunications Management Network
- TOS Type of Service
- TTL Time to Live
- UDP User Datagram Protocol
- VLAN Virtual Local Area Network (Virtual LAN)
- VPLS Virtual Private LAN Service
- VPN Virtual Private Network
- VPWS Virtual Private Wire Service
- VRF Virtual Routing and Forwarding instance
- VRRP Virtual Router Redundancy Protocol
- WAN Wide Area Network
- WFQ Weighted Fair Queuing
- WRED Weighted Random Early Detection

4 General requirements

4.1 The supplier shall deliver a fully functional Metro Ethernet equipment as a turnkey solution based on the Reference Architecture and BOQ.

4.2 The supplier shall study all SEC requirements and based on all facts propose a turnkey, cost effective solution, based on current international standards, including all necessary equipment (such as servers, power supply components, ancillaries, etc.)

4.3 Supplier shall be responsible to conduct a site survey to collect all relevant information that can have impact on project in terms of feasibility, BoQ items, cost, time plan and all aspects of realisation. Based on the site survey, the supplier shall propose all additional necessary equipment if any.

4.4 As per SEC requirements the supplier shall design the solution in such a way that it can provide efficient delivery of full range of services. This network shall be flexible and adjustable to future services, by proper dimensioning in design, hardware and software, to cope with services demands.

4.5 The Supplier shall produce a Solution Description (SD) document which will in detail explain functionality and design of each service, configuration of protocol and explanation of chosen options, benefits and drawback of solution as well as all possible limitations of that solution. SD shall extensively address resiliency and security threats, scenarios and protection solution. SEC will control and approve LLD through Technical Clarification list.

4.6 Shipment, custom clearance according to DDP (INCOTERMS2000) and delivery of all the equipment to the respective sites in KSA where the equipment will be installed.

4.7 The supplier's solution shall support all required retail, enterprise and wholesale product requirements specified in the SEC Product Offerings and Roadmap .

4.8 The supplier shall obtain all necessary certification from the KSA Telecoms Regulator for all equipment proposed in the solution prior to contract signing.

4.9 The supplier shall perform, or where performed by SEC, assist SEC in performing, and document user acceptance testing services for Applications developed implemented or modified by the supplier

4.10 The proposed solution will be according to the industry standards and based on supplier experience to provide the most effective and flexible network functioning. In exceptional cases, and with SEC's written agreement, proprietary standards may be used to achieve better capabilities.

4.11 The solution must be cost effective. It shall provide all necessary support for the services in chosen the design, and shall exclude unnecessary options that could increase the cost.

4.12 The solution must provide as best as possible performance of each proposed service.

4.13 All Hardware and software proposed to be deployed in SEC Network shall have at least 5 years roadmap guaranteed support. All relevant emerging technologies shall be clearly reflected in the roadmap.

4.14 The solution description document shall explain in detail the functionality and design of each service, the configuration of each protocol and full explanations of chosen options, the benefits and drawback of solution as well as all possible limitation of that solution

4.15 Services availability of 99.999% shall be assured by providing first class equipment with industry leading values for MTBF for the implemented HW and SW, and by providing redundancy features for hardware and proper configurations.

4.16 MTBF values shall be provided for all equipment

4.17 The solution shall offer enhanced security features and proper configuration of those options in the way that provide self-defending ability across whole network as well as per node basis.

4.18 Configurations of all network elements shall to be done in a way to provide a full set of features for all services mentioned in this RFP.

4.19 The proposed solution needs to incorporate effective and comprehensive tools for O&M through the deployment of appropriate EMS and NMS equipment to support Event and Fault

Management, Inventory Management, Configuration Management, Performance Management, Security and System Administration Management.

4.20 Supplier shall completely integrate Fault Management and other tools as required into existing SEC OSS platforms. The supplier shall offer the list of all possible alarms with alarm correlation indicated recommended action. SEC shall choose what needs to be forwarded to OSS.

4.21 The Supplier shall provide complete list of counters and recommendation for KPIs. SEC will choose what will be implemented.

4.22 The Supplier shall provide tools for collecting all relevant statistics from nodes that can be used for analysis and accounting.

4.23 The suppliers shall explain all the capacity and capability of the system offered and the relation to the unit price of each component of the system. This shall include hardware, software (port license, software license, etc), services and support, with the BoQ clearly linked to the pricebook.

4.24 The suppliers shall explain the right of SEC in using the license offered and the limitation in using the license. The suppliers shall also explain the capability and limitation of the existing NMS & License in performing all NMS function.

4.25 The Supplier shall propose usage based software licences wherever feasible (such as Pay As You Use, Pay As You Grow)

4.26 The suppliers shall indicate the conformance of the equipment to relevant international standards.

4.27 The suppliers shall guarantee the interoperability with other supplier equipment (including SDH, DWDM, Ethernet, IP equipment), any limitation/restriction with other suppliers shall be clearly defined in the technical document.

4.28 All hardware shall have 2 years free warranty

4.29 The supplier shall conduct a Proof of Concept (PoC) to demonstrate the solution to the requirements specified in this document

4.30 SEC shall not be responsible or liable for any costs incurred by the supplier in the PoC.

5 Product Offerings and Roadmap

5.1 The supplier’s proposed solution shall be able to provide a Metro Ethernet Network solution with appropriate, standards-based, quality of service.

5.2 The equipment shall support Service Provider infrastructure capabilities (e.g. support for Voice Media, Signalling and Management).

5.3 The equipment shall provide the following Layer 2 services: E-PL, EVPL, EP-LAN, EVP-LAN, EP-Tree, EVP-Tree, Access-EPL, Access-EVPL, PWE3, VPLS.

5.4 The Metro Area Network solution shall support L2 / L3 VPN's for businesses and residential voice, data, and multimedia services

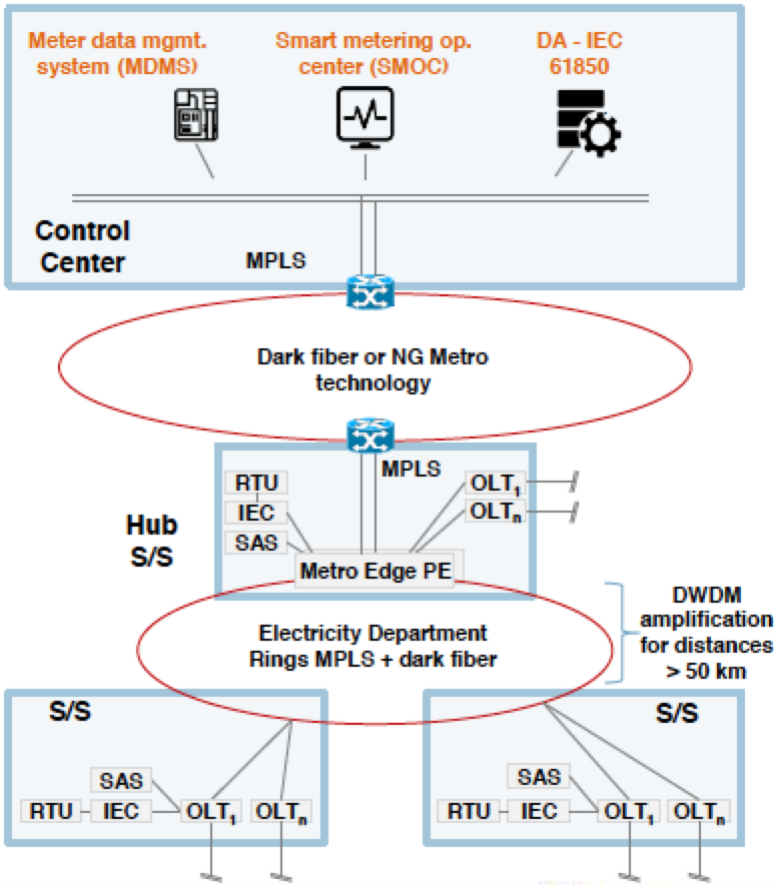
5.5 The Metro Area Network solution shall support planned Triple Play services such as Voice, High Speed Data, IPTV and Video-on-Demand.

5.6 The supplier's solution must be able to fulfil all SEC requirements for services at launch as well as future services.

6 Reference Architecture

6.1 The solution proposed by the Supplier shall conform with the requirements of the Reference Architecture Document, as indicated in Figure 1, which shows the Ethernet connectivity between substations (S/S) and hub substations:

Figure 1: High-Level Reference Architecture



6.2 The Aggregation network shall support Carrier Grade features in accordance with IEC 61850

6.3 The Aggregation network shall have the capability to interface with DWDM equipment, which may be required for distances beyond 50 km (for amplification)

6.4 The Ethernet equipment shall have full hardware redundancy and support for software redundancy

6.5 Every Metro Edge CE is connected point to point to 2 Metro Edge PE routers in the hub (for physical redundancy).

6.6 The Ethernet network shall support interfaces for 2 pairs of fibre per substation (e.g.18 fibre for 10 substation rings)

6.7 Supports for 1 Gigabit and 10 Gigabit Ethernet FO interfaces

7 Metro Ethernet Requirements

7.1 Overview

7.1.1 The supplier shall explain in detail the proposed solution taking into account the detailed requirements in this document, the technological concept and the service descriptions. The supplier shall clearly state if and where there is any deviation from the technological concept and why.

7.1.2 The supplier shall provide full details as to how carrier class availability is achieved, inclusive of but not limited to, the following aspects: hardware design (including backplane/system design and architecture), backplane capacity, software design and serviceability. This also includes availability analysis for the proposed network elements.

7.1.3 The system shall be fully integrated with its EMS/NMS

7.2 Hardware Requirements

7.2.1 Physical design shall be in low-profile (1-2 RU)

7.2.2 The supplier shall provide either 230 V AC or 48 DC power as required by the specific equipment

7.2.3 All elements shall be modular to allow for system expansion

7.2.4 System shall support IPV4 initially but running of Dual stack IPv4/IPv6 shall be possible to upgrade to IPv6.

7.2.5 Front to back cooling, hot swappable fan, and options for redundant power supplies shall be available.

7.2.6 Redundant Power supply capability shall be in built.

7.2.7 The equipment shall be installed in ETSI Racks

7.2.8 System shall support SNMP v3 access to the onboard SNMP agent.

7.2.9 System shall support standard optical SX/LX/ZX SFP or SFP+ but interoperability and support shall be ensured to allow other interconnected system and media.

7.2.10 The proposed hardware shall support the insertion and removal of interface and processing modules without causing any disruption to the system

7.2.11 The control (route processing, etc) and forwarding plane shall be physically separated on different modules

7.2.12 The control plane shall be redundant

7.2.13 All elements shall have wire speed performance

7.2.14 The typical delay for a packet to traverse a network element shall not exceed 10 µs

7.2.15 The elements shall have sufficient memory in order to satisfy current and future requirements

7.2.16 Each network element shall be provided with a local interface for a portable maintenance terminal.

7.2.17 The supplier shall state the maximum non-blocking, full duplex switching capacity of the proposed elements.

7.2.18 The supplier shall state the maximum packet size supported by the equipment and the packet forwarding speed at this maximum packet size.

7.2.19 The supplier shall supply datasheets as well as roadmaps for all the proposed hardware

7.3 Software requirements

7.3.1 The supplier shall propose software which has been proven under general release for no less than 18 months

7.3.2 The proposed software shall support a common command line

7.3.3 The proposed software shall be of a modular architecture

7.3.4 The proposed software shall support a software upgrade without a disruption of the forwarding plane (in-service upgrades)

7.3.5 The proposed software shall support a software upgrade without a replacement of hardware

7.3.6 The proposed software shall support a remote upgrade using TFTP or an equivalent protocol

7.3.7 The supplier shall include a bug impact analysis for the proposed software in the context of SEC's technological concept and service descriptions

7.3.8 The supplier shall provide datasheets as well as roadmaps for the proposed software.

7.3.9 The supplier shall provide information on his software release process at least for the next 3 years

7.4 Interface Requirements

7.4.1 The optical interfaces shall operate at 1310 nm or 1550 nm.

7.4.2 Optical transceivers shall be SFP-based (Small Form-Factor Pluggable) with interchangeable SC/LC optical connectors.

7.4.3 Automatic laser shutdown in accordance with ITU-T Rec. G.664 shall be implemented.

7.4.4 Automatic laser cut off shall be implemented

7.4.5 Automatic laser restart shall be implemented

7.4.6 Automatic laser cut off inhibition shall be implemented

7.4.7 Time limited manual laser restart shall be implemented

7.4.8 The supplier shall describe their solution to connect nodes that are to be connected by fibre optic cables with a cable length of more than 50km.

7.4.9 The supplier shall provide information regarding current state of development, applicability, deployment, upgradeability, and interoperability of/to/with client signals based on 100 Gbps and above.

7.5 Ethernet Interfaces

7.5.1 The proposed equipment shall support High-density configurations for the following optical Ethernet interfaces:

i. 10 Gbps Ethernet
ii. 1 Gbps Ethernet
iii. 100 Mbps Ethernet

7.5.2 The proposed interfaces shall support the following features:

i. A frame size larger than 2000 bytes
ii. 802.1q VLANs
iii. 802.1p COS
iv. 802.3ad link bundling
v. Disabling of STP or related protocols (e.g. RSTP, etc)

7.5.3 The supplier shall state for each of the proposed interfaces:

i. The supported Ethernet type (e.g. 802.3z 1000BASE-LX/LH)
ii. The maximum amount of supported VLANs
iii. The maximum amount of firewall-rules that can be supported
iv. The maximum amount of physical links that can take part in a single link bundle
v. The amount and type of hardware and software queues for QoS
vi. The amount of ports on a line-card (port density)

7.5.4 The supplier shall provide datasheets as well as a roadmap for the proposed interfaces

8 IP Addressing Requirements

8.1 General

8.1.1 The successful supplier shall create a detailed addressing plan according to SEC requirements.

8.2 IP version 4

8.2.1 All of the proposed systems must support IPv4 in hardware and software

8.2.2 In particular the following shall be supported:

i. IP version 4 (RFC 791)
ii. ICMP version 4 (RFC 792)
iii. TCP (RFC 793)
iv. UDP (RFC 768)
v. DNS client (RFC 1034 and RFC 1035)
vi. Path MTU discovery (RFC 1991)
vii. The software of the proposed equipment shall be implemented following RFC 1122.
viii. The supplier shall describe any deviation from RFC 1122

8.3 IP version 6

8.3.1 All of the proposed systems must support IPv6 in hardware and software

8.3.2 In particular the following shall be supported:

i. IP version 6 (RFC 2460)
ii. ICMP version 6 (RFC 2463)
iii. TCP (RFC 793 and RFC 2460)
iv. UDP (RFC 768 and RFC 2460)
v. DNS client
vi. IPv6 router alert option (RFC 2711)
vii. IPv6 jumbogram (RFC 2675)
viii. Path MTU discovery for IPv6 (RFC 1981)
ix. IP header compression (RFC 2508)
x. Security Architecture for the Internet Protocol (RFC 2401)
xi. Encapsulation Security Header (RFC 2402)
xii. IP Authentication Header (RFC 2406)
xiii. Neighbour Discovery Protocol (RFC 2461)
xiv. Extensions to IPv6 neighbour discovery for inverse discovery specification (RFC 3122)

8.3.3 The supplier shall explain how the proposed solution can be migrated to IPv6. The explanation shall include a list of systems that need hardware and/or software upgrades as well as an indication on the planning.

9 Quality of Service

9.1 General

9.1.1 The successful supplier must implement Quality of Service in accordance with the SEC requirements.

9.1.2 The supplier shall explain the proposed QoS concept in terms of classification, marking, policing and shaping. Special emphasize shall be placed on the capabilities and limitations of the proposed hardware and software.

9.1.3 The supplier shall explain the use of hierarchical QoS in the context of the SEC network

9.2 Classification

9.2.1 Classification of packets is required in order to determine to which class a particular flow belongs.

9.2.2 Ingress classification of packets shall be possible on a physical or logical port

9.2.3 Classification of packets based on the following parameters shall be supported for each of the proposed systems:

i. Source IP address
ii. Destination IP address
iii. Source TCP port
iv. Destination TCP port
v. Source UDP port
vi. Destination UDP port
vii. Protocol number
viii. DSCP Field
ix. TOS Field
x. MPLS EXP Field
xi. 802.1p TOS Field

9.2.4 The supplier shall explain how parameters are implemented in the proposed system and elaborate on the impacts on forwarding performance and CPU utilization.

9.3 Marking

9.3.1 Ingress marking of packets shall be possible on a physical or logical port

9.3.2 Marking of locally originated traffic (management and signalling traffic like routing protocols and telnet) shall be possible

9.3.3 The proposed systems shall support the following packet (re)markings:

i. DiffServ Field
ii. Type of Service Field
iii. MPLS EXP
iv. 802.1p TOS Field

9.4 Policing

9.4.1 Ingress policing shall be supported as follows:

i. Policing of Ethernet frames
ii. Policing of 802.1q VLANs
iii. Policing of IP packets

9.4.2 Policing shall support the following parameters:

i. CIR (Committed Information Rate)
ii. EIR (Exceeding Information Rate)
iii. MBS (Maximum Burst Size)

9.4.3 The supplier shall explain the limitations of the proposed hardware and software when policing is implemented on logical interfaces (e.g. 802.1q VLAN logical interface)

9.4.4 The supplier shall specify the minimum and maximum rate as well as the granularity of rate and burst tolerance.

9.4.5 The supplier shall specify the maximum number of simultaneously policed flows

9.4.6 The supplier shall explain the policing algorithms that can be used.

9.5 Shaping

9.5.1 Egress shaping shall be supported as follows:

i. Shaping of Ethernet frames
ii. Shaping of 802.1q VLANs
iii. Shaping based on a percentage

9.5.2 The proposed hardware and software shall support the following congestion management or queuing mechanisms:

i. Priority Queuing (PQ)
ii. Weighted Fair Queuing (WFQ)
iii. Class Based Weighted Fair Queuing (CBWFQ)
iv. Deficit Weighted Round Robin (DWRR)

9.5.3 The proposed hardware and software shall support the following congestion avoidance mechanisms:
- i. Random Early Detection (RED)
- ii. Weighted Random Early Detection (WRED)

9.5.4 The supplier shall explain the limitations of the proposed hardware and software when shaping is implemented on logical interfaces (e.g. 802.1q VLAN logical interface)

9.5.5 The supplier shall specify the maximum number of simultaneously shaped flows

10 Security Requirements

10.1 Security shall be implemented in order to ensure the availability, integrity and confidentiality of the network.

10.2 The supplier's solution must propose and implement security as required

10.3 It shall be possible to disable all un-needed services and routing protocols

10.4 It shall be possible to protect the control plane by means of filter lists

10.5 It shall be possible to restrict the traffic originated by and send to the control plane to predefined MAC addresses

10.6 It shall be possible to control user access to a device as follows:
- i. TACACS or RADIUS shall be used as the authentication protocol
- ii. Console access shall be disabled
- iii. Local authentication shall be disabled
- iv. Router management shall be done via SSH connections with SSH configured to authenticate with public key cryptography.

10.7 It shall be possible to implement a security banner

10.8 It shall be possible to timestamp all log entries using NTP time information

10.9 The supplier shall describe their approach to switch hardening.

11 Metro Ethernet Capabilities

Ethernet shall be used to carry SEC's traffic across the Aggregation and Access Network, either in combination with or in place of IP/MPLS. The supplier shall state their compliance against the latest international standards cover the following:

11.1 MEF 2 Requirements and Framework for Ethernet Service Protection

11.2 MEF 3 Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks

11.3 MEF 4 Metro Ethernet Network Architecture Framework Part 1: Generic Framework

11.4 MEF 6.2 EVC Ethernet Services Definitions Phase 3

11.5 MEF 7.2 Carrier Ethernet Information Model

11.6 MEF 8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks

11.7 MEF 9 Abstract Test Suite for Ethernet Services at the UNI

11.8 MEF 10.3 Ethernet Services Attributes Phase 3

11.9 MEF 10.3.1 Composite Performance Metric (CPM) Amendment to MEF 10.3

11.10 MEF 11 User Network Interface (UNI) Requirements and Framework

11.11 MEF 12.1 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer

11.12 MEF 13 User Network Interface (UNI) Type 1 Implementation Agreement

11.13 MEF 14 Abstract Test Suite for Traffic Management Phase 1

11.14 MEF 15 Requirements for Management of Metro Ethernet Phase 1 Network Elements

11.15 MEF 16 Ethernet Local Management Interface

11.16 MEF 17 Service OAM Framework and Requirements

11.17 MEF 18 Abstract Test Suite for Circuit Emulation Services

11.18 MEF 19 Abstract Test Suite for UNI Type 1

11.19 MEF 20 UNI Type 2 Implementation Agreement

11.20 MEF 21 Abstract Test Suite for UNI Type 2 Part 1 Link OAM

11.21 MEF 22.1 Mobile Backhaul Phase 2 Implementation Agreement

11.22 MEF 22.1.1 Amendment to MEF 22.1 – Small Cell Backhaul

11.23 MEF 23.1 Class of Service Phase 2 Implementation Agreement

11.24 MEF 24 Abstract Test Suite for UNI Type 2 Part 2 E-LMI

11.25 MEF 25 Abstract Test Suite for UNI Type 2 Part 3 Service OAM

11.26 MEF 26.1 External Network Network Interface (ENNI)–Phase 2

11.27 MEF 27 Abstract Test Suite For UNI Type 2 Part 5: Enhanced UNI Attributes & Part 6: L2CP Handling

11.28 MEF 28 External Network Network Interface (ENNI) Support for UNI Tunnel Access and Virtual UNI

11.29 MEF 29 Ethernet Services Constructs

11.30 MEF 30.1 Service OAM Fault Management Implementation Agreement Phase 2

11.31 MEF 30.1.1 Amendment to SOAM FM IA

11.32 MEF 31 Service OAM Fault Management Definition of Managed Objects

11.33 MEF 32 Requirements for Service Protection Across External Interfaces

11.34 MEF 33 Ethernet Access Services Definition

11.35 MEF 34 ATS for Ethernet Access Services

11.36 MEF 35 Service OAM Performance Monitoring Implementation Agreement

11.37 MEF 36.1 Service OAM SNMP MIB for Performance Monitoring

11.38 MEF 37 Abstract Test Suite for ENNI

11.39 MEF 38 Service OAM Fault Management YANG Modules

11.40 MEF 39 SOAM Performance Monitoring YANG Module

11.41 MEF 40 UNI and EVC Definition of Managed Objects (SNMP)

11.42 MEF 41 Generic Token Bucket Algorithm

11.43 MEF 42 ENNI and OVC Definition of Managed Objects (SNMP)

11.44 MEF 43 Virtual NID (vNID) Functionality for E-Access Services

11.45 MEF 44 Virtual NID (vNID) Definition of Managed Objects (SNMP)

11.46 MEF 45 Multi-CEN L2CP

11.47 MEF 46 Latching Loopback Protocol and Functionality

11.48 MEF 47 Carrier Ethernet Services for Cloud implementation Agreement

11.49 MEF 48 Service Activation Testing

11.50 MEF 49 Service Activation Testing Control Protocol and PDU Formats

11.51 MEF 49.0.1 Amendment to Service Activation Testing Control Protocol and PDU Formats

11.52 MEF 50 Service Operations Guidelines

11.53 MEF 51 OVC Services Definitions

12 Element and Network Management Systems

12.1 General

This section of the document addresses requirements for the resource management layer of the BSS/OSS architecture for the packet core network of this project.

12.1.1 In reference to the Telecommunications Management Network Model (TMN), the supplier shall provide network management for the Resource Management Layer consisting of element management and network management.

12.1.2 The proposed NMS shall be capable of being integrated into, and compatible with SEC's resource management layer in the OSS architecture

12.1.3 The supplier shall propose a single EMS to manage the equipment offered in response to this RFP.

12.1.4 The Element Management Layer offered by the supplier shall provide the management functionalities at the NE Level from a central application able to control a set of equipment.

12.1.5 The proposed solution shall provide full Layer 2 management fuctionality

12.2 Interfaces of EMS to the resource management layer

12.2.1 The EMS shall support configuration, fault, testing, performance and administration management.

12.2.2 The EMS shall interface with the existing resource inventory management in order to transfer inventory data.

12.2.3 The EMS shall interface with existing resource activation in order to exchange configuration data.

12.2.4 The EMS shall interface with existing resource data collection management in order to exchange status, performance, testing, alarm data.

12.2.5 The management system shall support a configuration management in a way that it comprises network element configuration and provisioning, network configuration and reconfiguration, traffic set-up.

12.2.6 The management system shall support set up of end to end services with a point and click and definition of A-Z points

12.2.7 Services provisioning shall be performed and fully controllable from the NMS GUI

12.2.8 The management system GUI shall support route display for infrastructure and services, showing the correlation between services, network elements and cards, with associated alarms indicated in the routing. MIP and MEP maintenance domains shall be supported in accordance with IEEE 802.1ag

12.2.9 The operation of the system shall be integrated, with a one-click navigation between lists, alarms, performance management, and routing display

12.2.10 The management interface between the Gateway Network Element GNE and the EMS shall be based on SNMPv3.

12.3 Specific functional requirements to the NMS/EMS

This section describes in more detail the desired functions for the different network management such as management of fault, configuration, administration, and performance.

12.3.1 Fault Management

12.3.1.1 The supplier shall list the alarms monitored for each NE type

12.3.1.2 The proposed EMS of the network elements shall be compatible with the existing OSS solution

12.3.2 Configuration Management

12.3.2.1 The NMS system proposed shall provide configuration functions for construction management (network topology), NE management, and software management.

12.3.2.2 The configuration management function shall deal with the topology of the network as seen from the graphical user interface. It shall provide, at a minimum, the following functionality: declaring a topology, adding or removing symbols (sites, NE's, connections) from a declared topology, declaring NE's, and NE inventory.

12.3.2.3 The NE management function shall provide, at a minimum, the following functionality for the equipment present in the network: configuration of NE's, supervision of NE's, changing of boards, configuration of the protection schemes (in case of equipment failure), allow/Inhibit alarm notifications and configuration of the alarm severity profile

12.3.2.4 The SW management function refers to the software package(s) present in the NE. It shall provide, at a minimum, the following features: accessing

information about the software package(s) downloaded in a selected NE, downloading software packages from a remote server to an NE, activating/deactivating software packages, and committing software packages.

12.3.2.5 Software download or software upgrade shall not affect any traffic in the associated network.

12.3.2.6 The supplier shall describe in detail the systems functionality in traffic engineering and QoS profile management.

12.3.2.7 There shall be an embedded consistency check of the management system database against predefined network element configuration files to highlight any possible misalignment and raise an alarm if necessary

12.3.2.8 Configuration changes shall be pushed from a central system to the different network elements or groups of network elements

12.3.2.9 Configuration changes shall be compared to predefined configuration templates before implementing the changes. In case of a deviation from the template, a confirmation pop-up window shall be raised, allowing the operator to refuse the configuration change;

12.3.2.10 It shall be possible to schedule configuration changes for implementation in out-of-business hours;

12.3.2.11 The described functions shall be compatible with further requirements of the existing OSS

12.3.3 Performance Management

12.3.3.1 The supplier shall describe the performance parameters which can be monitored in the NE's and in particular the external probes.

12.3.3.2 The performance management shall be capable of processing data received from the network elements such as CPU utilization, memory utilization, latency, jitter and packet loss.

12.3.3.3 The NMS shall be capable of generating reports

12.3.3.4 The NMS shall be capable of periodically collecting, presenting, and storing performance data from the managed NE's.

12.3.3.5 The supplier shall describe the performance parameters which can be monitored using the proposed system

12.3.3.6 The supplier shall describe all performance parameters, which may be collected from the NE's.

12.3.3.7 The described functions shall be in compliance with, and compatible with further requirements of the existing OSS/BSS

12.3.4 Administration

12.3.4.1 At EMS level, database protection with disk mirroring technique is required, while HW duplication is required at NMS Layer.

12.3.4.2 Alarm logs and system logs shall be archived to secondary storage automatically under predefined mechanism and shall be browsed on-line.

12.3.4.3 System log (Syslog) shall be available for export to an external system

12.3.4.4 The described functions shall be compatible with further requirements of the existing OSS

12.3.4.5 The management information flow between all other network elements and EMS/NMS shall be possible via a management VPN, if required.

12.3.5 Integration/Compatibility

The following constraints in respect to integration and compatibility have to be matched by the proposed system.

12.3.5.1 The supplier shall describe their capabilities related to the integration of their NMS with NMS and EMS of different suppliers in a multi-vendor environment.

12.3.5.2 The supplier shall provide a description of the proposed system including, but not limited to: architecture, reference information model, level of integration supported, and standards compliance.

12.3.5.3 The supplier shall ensure interoperability of their solution with the overall BSS/OSS/NMS solution.

13 Operating Conditions

13.1 All equipment specified shall be capable of an operating normally in the temperature range -5 to 40 °C

13.2 All equipment specified shall be capable of being stored without impact to performance in the temperature: -20 to 70 °C

13.3 All equipment specified shall be capable of an operating normally in the humidity range: 20 to 95% non-condensing

14 Network Reference

14.1 Supplier shall submit at least TEN Metro Ethernet network references, which shall be installed and with live traffic with the Network restoration feature being implemented.

15 Installation

15.1 The Supplier shall be responsible for a full installation of all equipment on site which includes mounting into the racks, cabling in MDF, power cabling etc and if required installation of rectifiers, DB, batteries, etc as a turnkey solution.

15.2 The Supplier shall be responsible for full configuration of all protocols, features and options thereby providing optimal performance of system, preserve processing resources and implement all relevant security standards and protection mechanisms related to deployment scenario.

15.3 The Supplier shall as part of the project fully integrate their solution into SEC existing systems, from network to applications level (supporting existing products and services)

15.4 The shall be responsible for the installation and/or integration of a Network Management System, including configuration and integration of all network elements included in the solution into NMS. NMS shall provide full functionality for Fault Management, Topology Map, Configuration, Performance and Security Management. Performance and Fault management will be based on SEC recommendations and inputs from the supplier's experience. Supplier shall provide list of all counters and alarms that the equipment supports.

15.5 Integration of FM (alarms and traps) into existing OSS for all proposed components through central management node.

15.6 Configuration of all components in a legible manner thereby providing templates for plug and play of all services

15.7 Detailed as built documentation covering all aspects of the installation and detailed operational procedures.

16 Testing and inspection

16.1 The Supplier shall perform full functional tests, including verifying the establishment of stable and quality connections end to end

16.2 The supplier shall be required to demonstrate results of the following standard MEF test suites:

16.2.1 MEF 9 Abstract Test Suite for Ethernet Services at the UNI

16.2.2 MEF 14 Abstract Test Suite for Traffic Management Phase 1

16.2.3 MEF 18 Abstract Test Suite for Circuit Emulation Services

16.2.4 MEF 19 Abstract Test Suite for UNI Type 1

16.2.5 MEF 21 Abstract Test Suite for UNI Type 2 Part 1 Link OAM

16.2.6 MEF 24 Abstract Test Suite for UNI Type 2 Part 2 E-LMI

16.2.7 MEF 25 Abstract Test Suite for UNI Type 2 Part 3 Service OAM

16.2.8 MEF 27 Abstract Test Suite For UNI Type 2 Part 5: Enhanced UNI Attributes & Part 6: L2CP Handling

16.2.9 MEF 37 Abstract Test Suite for ENNI

16.2.10 MEF 48 Service Activation Testing

16.2.11 MEF 49 Service Activation Testing Control Protocol and PDU Formats

16.2.12 MEF 49.0.1 Amendment to Service Activation Testing Control Protocol and PDU Formats

16.3 All tests shall perform all tests in the presence of SEC designated witnesses

16.4 Provisional Acceptance Test (PAT) and Final Acceptance Test (FAT) procedures must be documented and network acceptance will be performed based on the proposed tests and validated against the expected results.

16.5 Supplier shall assist with the development of user acceptance test plans and acceptance criteria for approval by SEC.

16.6 Supplier shall assist SEC to develop and document test cases for user acceptance testing.

16.7 Supplier shall assist SEC to coordinate user acceptance testing, including identification and support for all Authorized Users participating in the testing.

16.8 Supplier shall perform the Acceptance Testing operation, including project management, test planning, design and execution. All process are designed to fully address the business requirements and match SEC customer needs

16.9 Prior to SEC UAT, the Supplier will certify that it has completed internal testing on the entire solution and that all software delivered for UAT shall be free of defects and pass the same tests when administered by SEC staff.

16.10 The Supplier is required to perform the tests for the system to demonstrate the Acceptance Test Procedure KPIs.

16.11 The acceptance test scenarios shall aim to simulate the real live processes. A major part of this complexity will be derived from the data. Therefore, the AT shall be executed with production data, not synthetic data.

16.12 Supplier shall ensure all important aspects are ready for the UAT execution stage. This shall be done according to a checklist with pre-defined quality gates. This checklist will be finalized in consultation with SEC during the AT-Plan phase.

16.13 Manage and control the changes in the contents of the environments: The tested software, interfaces, reference data, and business data.

16.14 The Test Execution phase shall contain few rounds, depending on the system scope. Each round may have a different scope. Test Scenarios are to be executed in parallel on multiple UAT environments, in order to be efficient and monitor progress in several areas.

16.15 The entire Acceptance Test scope shall include new functionality, regression, defects, interfaces, business processes, and non-functional testing.

16.16 Prior to PAT, the Supplier shall handover all documentation as may be required by SEC, including as-built diagrams and O&M documentation