INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

16885-C118 (181022)

Study Group 13

English only

Question(s):	Q19/13	Switzerland [Geneva], 2018-10-22/11-02

RAPPORTEUR GROUP MEETING – C

Source:	India
Title:	Y.e2efapm-reqts - Proposal for addition of functional requirements related to end-to-end fault and performance management of virtual network services under the clause 8
Purpose:	Proposal

Contact:	Lav Gupta DOT India	Tel: + 13148250063 Fax: + 919868217055 E-mail: lavgupta@wustl.edu
Contact:	Mahabir Parshad TEC DOT India	Tel: +919868217055 Fax: +91 11 23329088 E-mail: srddg.tec@gov.in
Contact:	Arvind Chawla TEC DOT India	Tel: +91 9868512165 Fax: +91 11 23714866 E-mail: arvind.chawla@gov.in
Contact:	Sridhar Sapparapu TEC DOT India	Tel: +919013133805 Fax: +91 11 23329062 E-mail: diri.tec@nic.in
Contact:	Uttam Chand Meena TEC DOT India	Tel: +919013131137 Fax: +91 11 23329062 E-mail: adetit.tec@gov.in
Contact:	Yan Lei Datang Software Technologies CO.,LTD. CHINA	Tel:+86 10 58917778 Email:yanlei03@datang.com

Keywords: Fault, performance, alarm generation, correlation, correction, root cause

Abstract: This contribution proposes to add functional requirements related to end-to-end fault and performance management of virtual network services under the clause 7 of Draft Recommendation Y. e2efapm-reqts.

1. Proposal

This contribution proposes to add functional requirements related to end-to-end fault and performance management of virtual network services under the clause 7 of Draft Recommendation Y. e2efapm-reqts.

8. Framework of end-to-end fault and performance management of virtual network services in inter-cloud

[Contributor’s note] This clause will provide framework of end-to-end fault and performance management of virtual network services in inter-cloud. At the moment, existing material is illustration only and allows better positioning aspects of virtual network services in general network architecture. This material will be updated accordingly. Contributions are invited.

8.1 CCRA framework

The functional components of the cloud computing reference architecture (ITU-T Y.3502) is as given below.

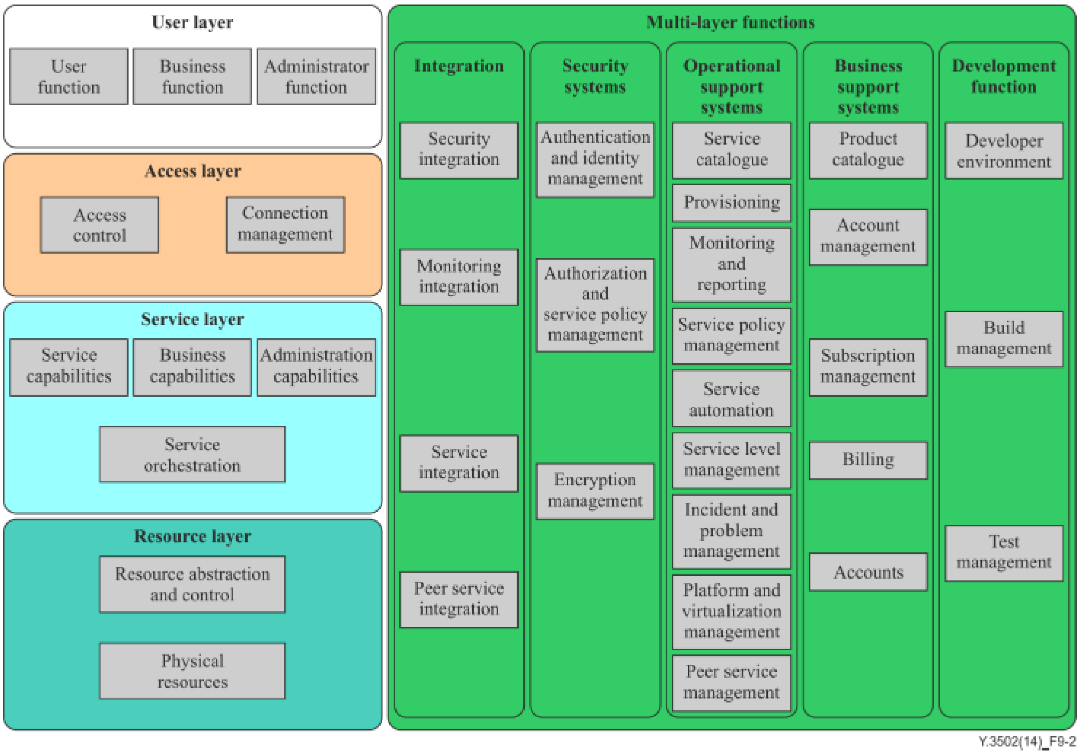


Figure- Functional components of CCRA

The fault and performance detection and localization model specified in para 8.7 is applied to the above CCRA. The individual layers containing the different functions of the model above are as depicted below.

8.2 **Fault management framework in resource layer**

The two functional components, viz physical resources and resource abstraction and control, available in the resource layer generate various alarms pertaining to the physical resources and virtual resources.

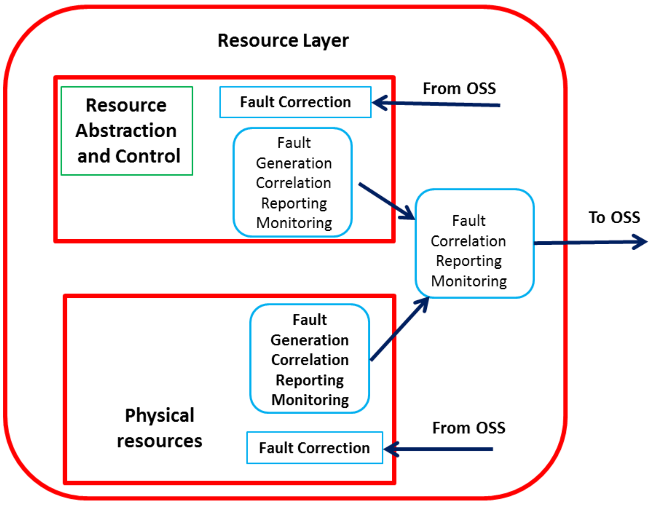

Resource Layer
Resource Abstraction and Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Physical resources
Fault Correction
From OSS

Figure- Fault management framework in resource layer

The physical resources such as the servers, networking switches and routers, storage devices generate the alarms/errors/faults during abnormal/failure conditions. When a network interface card/network link provides degraded performance, all the CPUs/cores attached to this card/link also provide degraded performance as the data received from NID/network link is erroneous. The host operating system or the virtualisation software lying above these physical resources needs only to respond to the root cause so that suitable action can be taken by it instead of reacting to every alarm generated from all the CPUs/Cores. Thus the alarms generated by various physical resources are required to be correlated and the probable causes of the alarms are to be identified and reported.

The software elements or virtual resources such as virtual machines (VM), virtual data storage etc., that can include in the resource abstraction and control functional component may generate alarms during their life cycle management. The multiple alarms related to a single virtual resource and similar alarms related to multiple virtual resources are required to be correlated in this functional component. For eg: The cloud work loads working on multiple VMs assigned with the same physical storage unit may underperform in case the RAID system on that storage unit fails. Instead of shifting the cloud work loads on different VMs as the present VMs are not delivering the desired resource performance, assigning a different storage unit may resolve the root cause. Thus the alarms generated by various software elements in this layer are required to be correlated and the probable causes of the alarms are to be identified and reported.

The alarms from both the above functional components are required to be correlated and the root cause alarm is required to be reported to resource fault management module of OSS.

Based on the automated policies and/or based on the direction from OSS, fault correction module in each of the functional components endeavours to rectify the fault in respective functional component.

8.3 **Fault management framework in service layer**

The service layer contains four functional components of which two components relevant from fault generation and management perspective are shown in the figure. These two components are service capabilities and service orchestration.

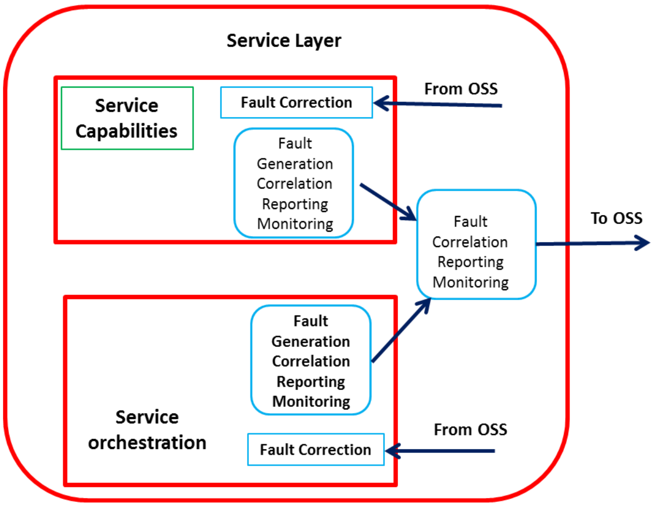

Service Layer
Service Capabilities
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Service orchestration
From OSS
Fault Correction

Figure- Fault management framework in service layer

The service implementation software, which creates the service using the under lying software elements (VMs, Virtual storage etc.,) in Service Capabilities functional component, may generate vide range of alarms/faults. This software generate the faults/alarms such as service creation failure, insufficient software elements, VNF failure, VNF software failure, VNFC failure, VNFC software failure, VNFFG error, etc. In case multiple VNF instances working in a NFVI-PoP fail this functional component may generate VNF software failure alarm. However, by correlating with multiple VNF instances working in another NFVI-PoP, VNF software failure or under lying software elements error can be identified. Thus alarms from various services and software implementing the service are to be correlated and the root cause of the alarms is required to be identified.

The service orchestration functional component provides coordination, aggregation and composition of multiple service components in order to deliver the cloud service. Alarms are generated by various service failures during the life cycle management of the services. The multiple alarms related to a single service and similar alarms related to multiple services are required to be correlated in this functional component.

The alarms from both these functional components are required to be correlated and the root cause alarm is reported to service fault management module of OSS.

8.4 **Fault management framework in access layer**

The two functional components, viz., Access control and connection management, in the resource layer also generate the alarms during the authentication, authorisation and SLA monitoring etc.

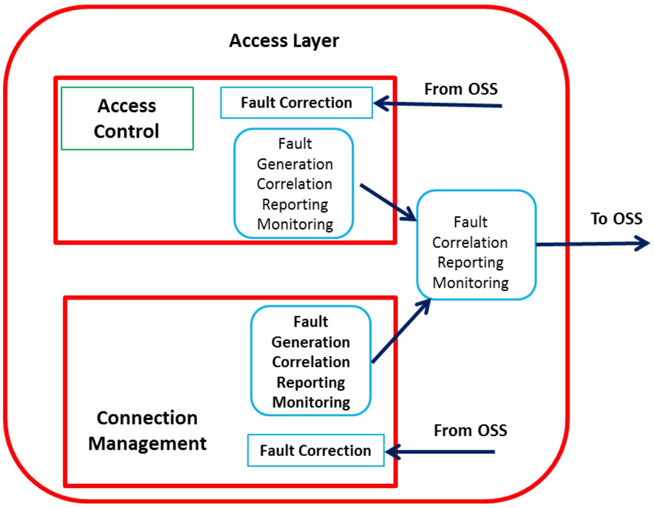

Access Layer
Access Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Connection Management
From OSS
Fault Correction

Figure- Fault management framework in access layer

The access control include the authentication of users and authorisation of authenticated users to use specific service. This functional component generate the alarms such as access denied, authentication failed, invalid credentials etc. These alarms are required to be correlated and the root cause of the alarms is identified.

The connection management provides enforcement of QOS policies. Alarms generated by this component may include such as no traffic, traffic failed, overload, under loaded etc. The multiple alarms related to a single CSC and similar alarms related to multiple CSCs are required to be correlated in this functional component.

The alarms from both the functional components are required to be correlated and the root cause alarm is reported to access fault management module of OSS.

Based on the automated policies and/or based on the direction from OSS, fault correction module endeavours to rectify the fault in respective functional component.

8.5 Fault management framework in a single cloud

The figure below shows the high level concept of fault management using CCRA functional components. For the purpose of simplicity of the 5 multi layers only OSS layer is shown.

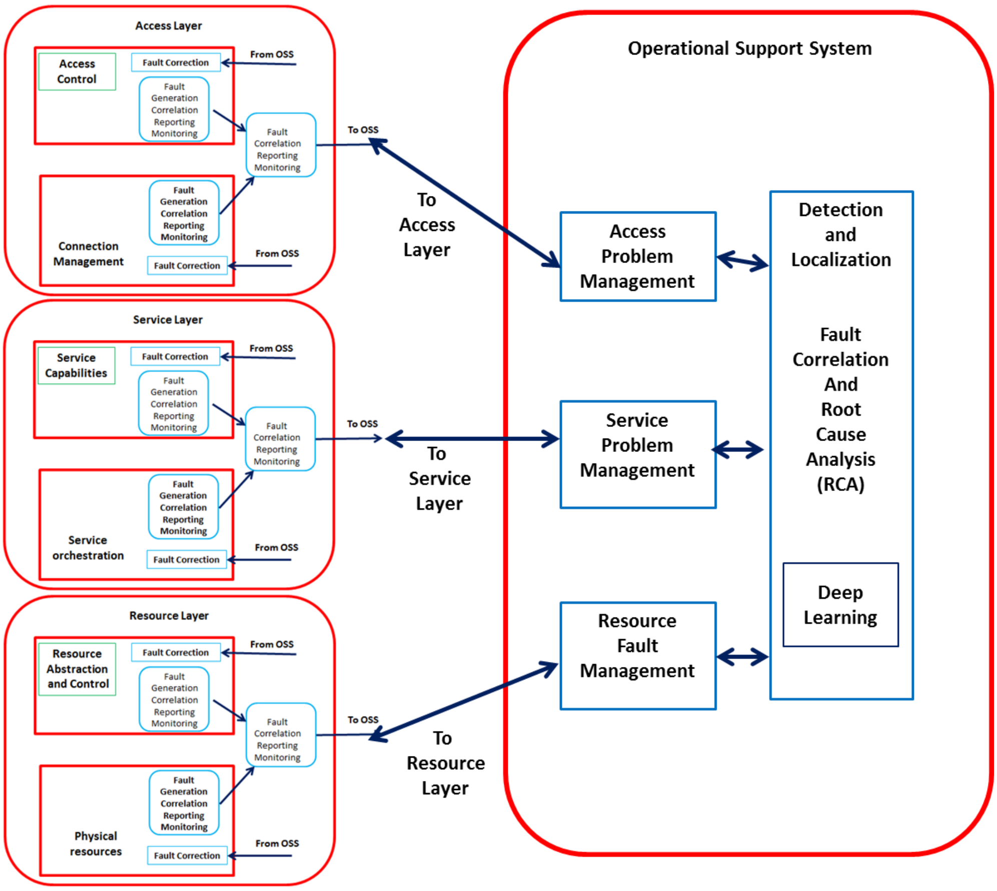

Access Layer
Access Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Connection Management
From OSS
Fault Correction
Service Layer
Service Capabilities
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Service orchestration
From OSS
Fault Correction
Resource Layer
Resource Abstraction and Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Physical resources
From OSS
Fault Correction
To Access Layer
To Service Layer
To Resource Layer
Operational Support System
Access Problem Management
Service Problem Management
Resource Fault Management
Detection and Localization
Fault Correlation And Root Cause Analysis (RCA)
Deep Learning

Figure – Fault management in CSP domain – Single cloud

In para 8.3 of ITU-T Y.3521 the management layers are defined as given below.

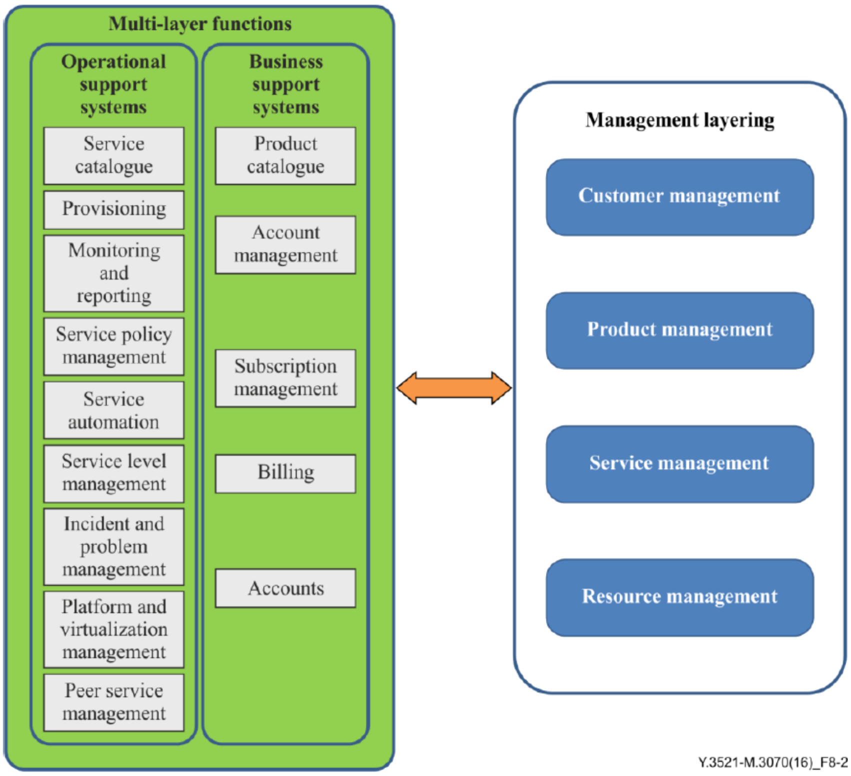
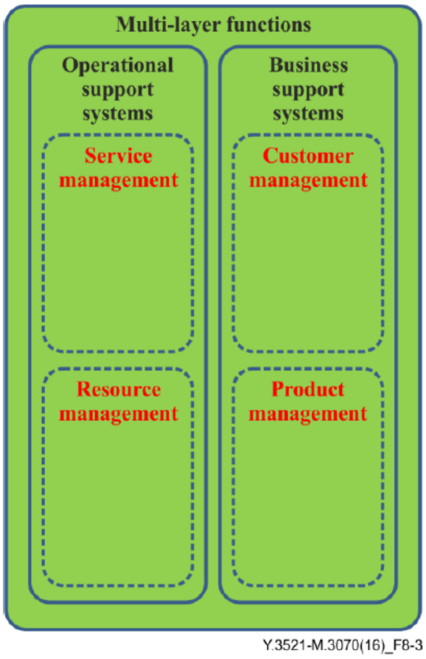


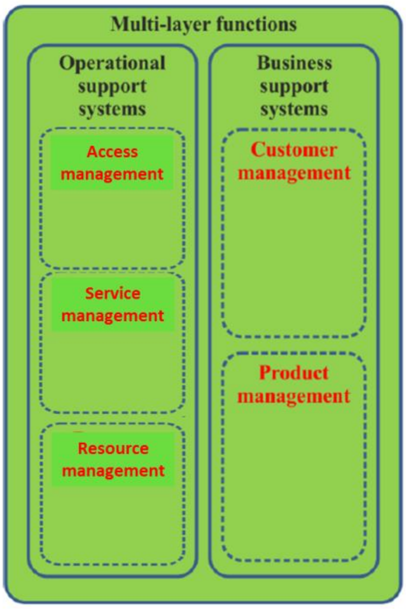
Figure- Relationship of OSS/BSS and management layers

In Figure 8.3 of ITU-T Y.3521 the management layers are mapped to OSS/BSS components as shown below.

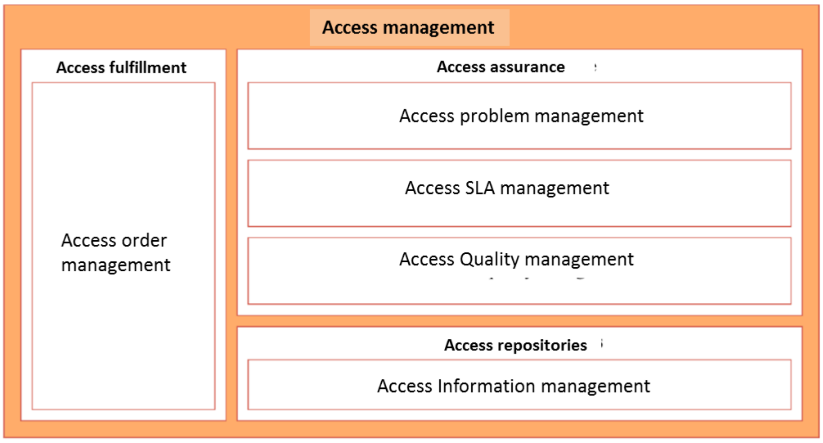


However, the access layer which is part of the functional components of CCRA is not included in the above diagrams. As the access layer is important from the fault management perspective, it is recommended that access management may be made a part of the management layers in addition the four layers already defined.

Considering this the management layers are suggested as given below.



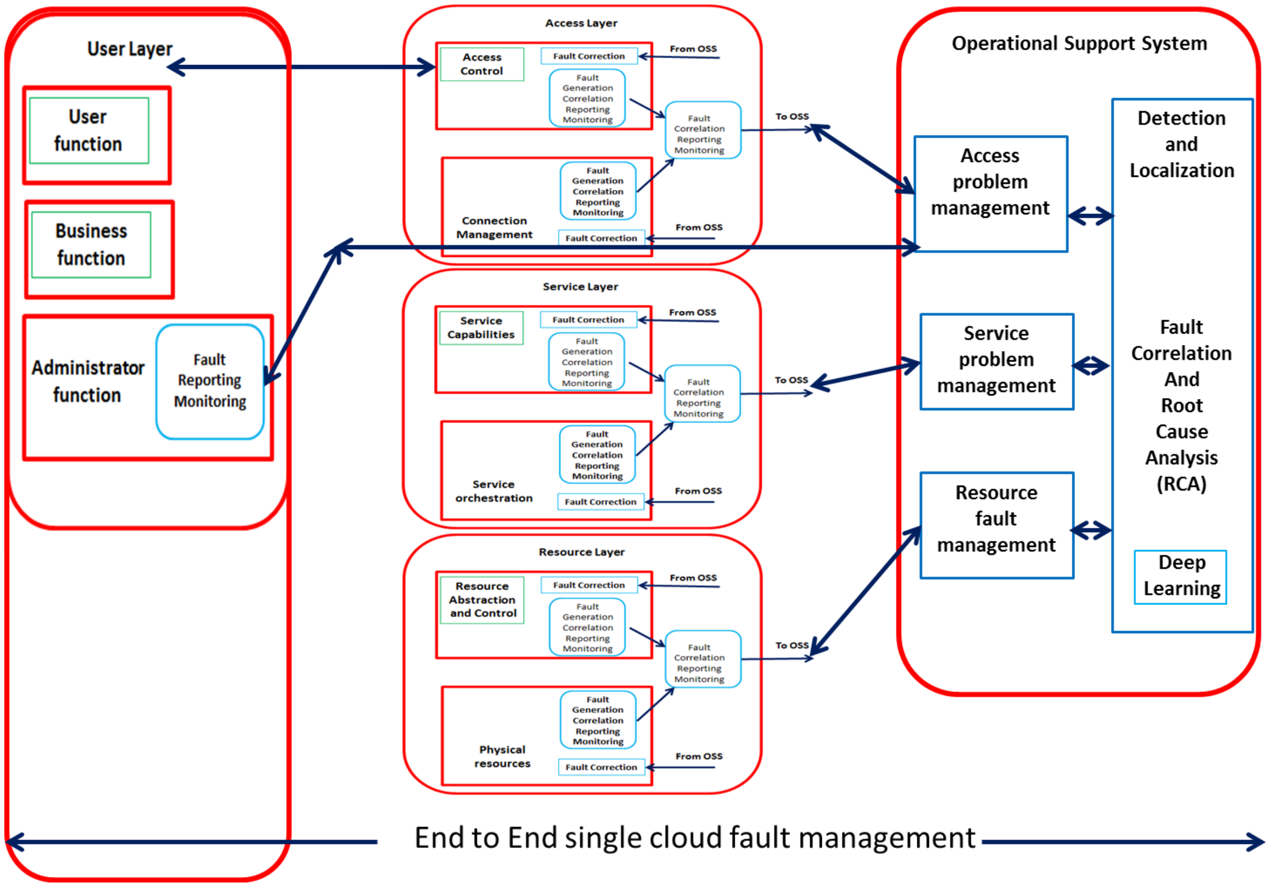
The access management is suggested as given below.



Accordingly, the CCRA model is adopted as per this suggestion in para 8.5 above.

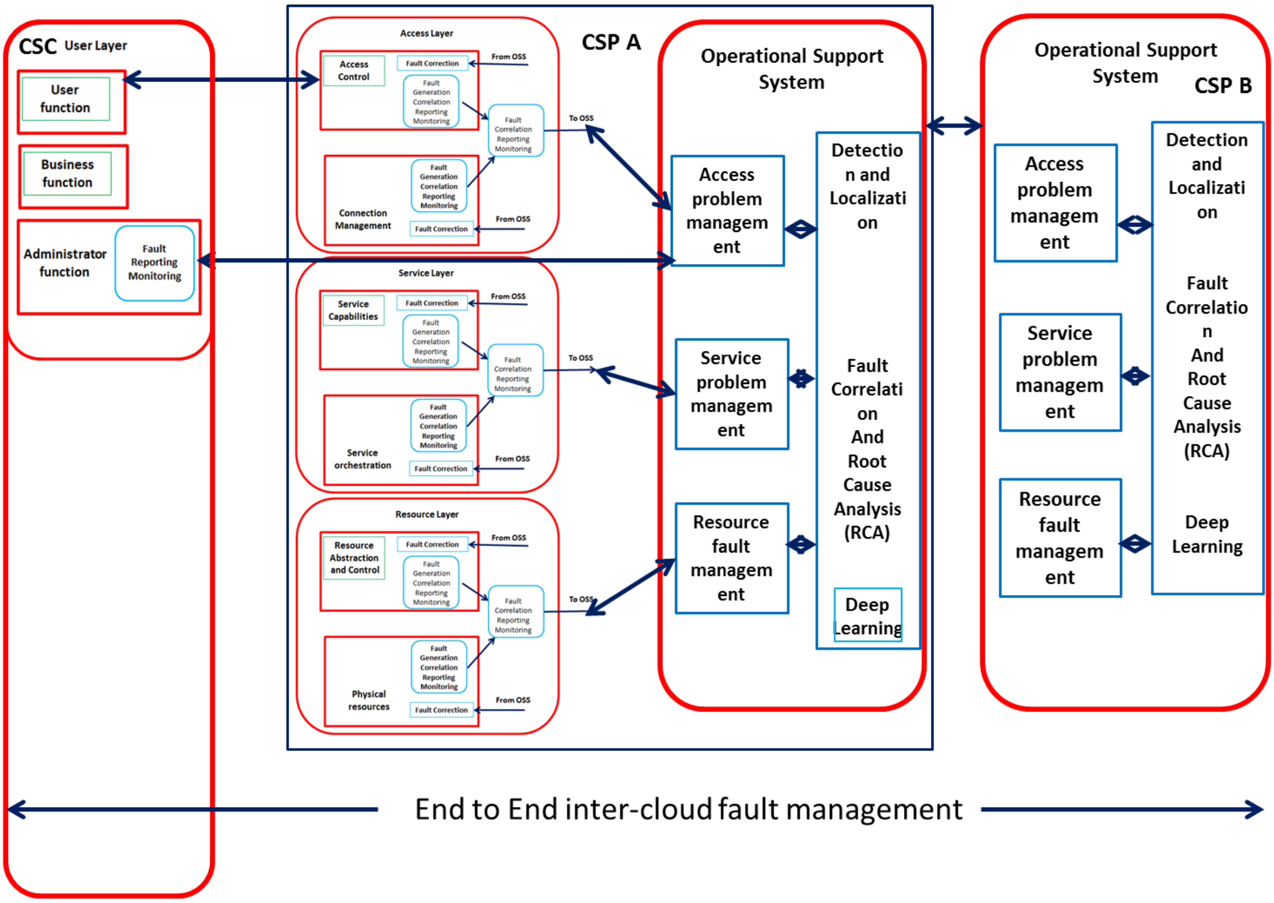
8.5 End to End Fault management framework in a CSP or a Single cloud

The End-to-end fault management framework in a CSP/single cloud is as shown below.


User Layer
User function
Business function
Administrator function
Fault Reporting Monitoring
Access Layer
Access Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Connection Management
Fault Correction
From OSS
Service Layer
Service Capabilities
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Service orchestration
Fault Correction
From OSS
Resource Layer
Resource Abstraction and Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Physical resources
Fault Correction
From OSS
Operational Support System
Access problem management
Service problem management
Resource fault management
Detection and Localization
Fault Correlation And Root Cause Analysis (RCA)
Deep Learning
End to End single cloud fault management

8.6 End to End Fault management framework in inter-cloud

The End-to-end inter-cloud fault management framework is as shown below. The primary CSP, CSP A provides virtual network services to the CSC. The CSP A also avails the virtual etwork services from CSP B. The three layers (Access, service and resource) of CSP B are also part of the end to end fault management. For the purpose of simplicity the three layers of CSP B are not depicted in the figure below.


CSC
User Layer
User function
Business function
Administrator function
Fault Reporting Monitoring
Access Layer
CSP A
Access Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Connection Management
Fault Correction
From OSS
Service Layer
Service Capabilities
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Service orchestration
Fault Correction
From OSS
Resource Layer
Resource Abstraction and Control
Fault Correction
From OSS
Fault Generation Correlation Reporting Monitoring
Fault Correlation Reporting Monitoring
To OSS
Fault Generation Correlation Reporting Monitoring
Physical resources
Fault Correction
From OSS
Operational Support System
Access problem managem ent
Service problem managem ent
Resource fault managem ent
Detectio n and Localizati on
Fault Correlati on And Root Cause Analysis (RCA)
Deep Learning
Operational Support System
CSP B
Access problem managem ent
Service problem managem ent
Resource fault managem ent
Detection and Localizati on
Fault Correlatio n And Root Cause Analysis (RCA)
Deep Learning
End to End inter-cloud fault management

____