|  |
| --- |
| Fault Diagnostics and Maintenance Functional Description |
| Date: 2016-01-21 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Hao Wang | Fujitsu R&D Center | +86-10-59691000 | wangh@cn.fujitsu.com |
| Su Yi | Fujitsu R&D Center | +86-10-59691000 | yisu@cn.fujitsu.com |
| Xiaojing Fan | Fujitsu R&D Center | +86-10-59691000 | fanxiaojing@cn.fujitsu.com |
| Ryuichi Matsukura | Fujitsu/Fujitsu Laboratory | +81-44-754-2667 | r.matsukura@jp.fujitsu.com |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document proposes initial text for the function of fault diagnosis and maintenance within Functional Design and Decomposition.

7 Functional Decomposition and Design 3

7.8 Fault Diagnostics and Maintenance (FDM) 3

7.8.1 Introduction 3

7.8.2 Roles and identifiers 4

7.8.3 Use Cases 5

7.8.3.1 Link FDM I 5

7.8.3.2 Link FDM II 6

7.8.3.3 Path FDM 7

7.8.4 Functional Requirements 8

7.8.5 FDM specific attributes 8

7.8.5.1 Terminal 8

7.8.5.2 Node of Attachment 8

7.8.5.3 Access Network Controller 8

7.8.5.4 Backhaul 8

7.8.5.5 Access Router 9

7.8.6 FDM specific basic functions 9

7.8.6.1 Capability discovery 9

7.8.6.2 Remote failure indication 9

7.8.6.3 Link monitoring 10

7.8.6.4 Remote test 10

7.8.6.5 Aggregation 11

7.8.6.6 Failure Isolation 11

7.8.6.7 Fault recovery 12

7.8.7 Detailed procedures 12

7.8.7.1 Remote failure indication 12

7.8.7.2 Link monitoring 13

7.8.7.3 Remote test 13

7.8.7.4 Aggregation 14

7.8.8 Mapping to IEEE 802 Technologies 15

7.8.8.1 Overview 15

7.8.8.2 IEEE 802.3 specifics 15

7.8.8.3 IEEE 802.11 specifics 15

7.8.8.4 IEEE 802.16 specifics 15

7.8.8.5 IEEE 802.22 specifics 15

# Functional Decomposition and Design

## Fault Diagnostics and Maintenance (FDM)

### Introduction

Fault diagnosis and maintenance (FDM) provides the capabilities for detecting, isolating, reporting and mitigating the failures during the life cycle of network session. These capabilities allow the network operators as well as the service providers to monitor the health of the network and quickly determine the location of failing links or fault conditions, and take necessary measures to recover the faults.

Fault denotes a deviation of a system from normal operation, which may result in the loss of operational capabilities of the element or the loss of redundancy in case of a redundant configuration. A fault may occur on a network entity, cause the malfunction of the logical and physical resources and will, in severe cases, lead to the complete unavailability of the respective network entity. A fault may also occur on a link and cause communication performance deterioration, thus affect quality of service. Besides, a fault may occur along a data path which is established to carry user payload between the terminal and access router, or between the terminal and another terminal, and affects the end-to-end connectivity.

In a local network scenario as defined by IEEE Std 802.11, instances of the faults that may affect the communication or connection in the transmission between the AP and station include the problem of a unit failure of the AP and station that establish communication; the problem of a setup mistake; the problem of the radio channel used; and the problem of radio propagation that mainly affects the propagation of signals.

As a consequence of faults, the appropriate alarms related to the physical or logical resources affected by the faults, shall be generated by a network entity. An alarm signifies an undesired condition of network resource that can be grouped into one of the following categories:

* communications alarm type: An alarm of this type is principally associated with the procedures and/or processes required to convey information from one point to another;
* quality of service alarm type: An alarm of this type is principally associated with a degradation in the quality of a service;
* processing error alarm type: An alarm of this type is principally associated with a software or processing fault;
* equipment alarm type: An alarm of this type is principally associated with an equipment fault;
* environmental alarm type: An alarm of this type is principally associated with a condition relating to an enclosure in which the equipment resides.

Regarding the context where FDM is used, FDM functions are described on two levels, i.e. link level and path level.

Link FDM is conducted on a link involving both connected entities, intends to detect faults as soon as they occur and to limit their effects on the network Quality of Service (QoS) as far as possible.

Path FDM is conducted towards a data path involving multiple entities, intends to discover and verify the path through bridges and LANs, to detect and isolate of a connectivity fault.

The following concepts are introduced to support multiple independent operators, each supporting service instances for multiple independent customers:

* Maintenance domain is a management space of a network that is controlled by a single operator and used to support connectivity between network entities.
* Maintenance domain intermediate point (MEP) is at the edge of the domain, which defines the boundary for the domain. MEP can generate and receive path FDM messages and track any responses.
* Maintenance domain intermediate point (MIP) is internal to a domain and can react to some path FDM messages. MIPs can add, check, and respond to information in received path FDM messages, thus supporting discovery of paths among MEPs and location of faults along those paths.

How to configure MEPs and MIPs are dependent on business models and deployment scenarios.

Figure 7-8-1 gives a simple illustration on maintenance domain, MEP, and MIP in path FDM. Customer/provider/operator domains are defined by operational or contractual boundaries.



Figure 7-8-1: Maintenance Domain, MEP, and MIP

Network entities may be involved in both link FDM and path FDM at the same time. As different FDM functions performed simultaneously by one entity, and FDM decisions or results are derived from separate link FDM and path FDM. In some cases, link FDM and path FDM interworking can be supported to achieve better fault diagnostic performance.

### Roles and identifiers

The control entity contained by TE, AN and AR facilitates the FDM functions according to its configurations and capabilities.

In order to detect faults, the controllers may use autonomous self-check circuits and measurement procedures to observe the performance of physical ports.

Interfaces between controllers, i.e R8, R9, are used to exchange necessary FDM information for basic functions, e.g.

* configure the parameters, threshold and FDM process of a remote entity
* notify the alarms of detected fault to a remote entity
* aggregate FDM related information from a remote entity
* control a remote entity to enter test mode to execute the testing procedure which may involve a third party entity

As soon as an entity enter the test mode, data interfaces, i.e R1, R6, and R3 will be used to carry test messages to obtain more detail information.

When the comprehensive reference model is applied, the control interfaces within the access network, i.e. R5/R7 is used respectively for configuration and operation of the NA and BH, e.g.

* monitor the communication performance of physical ports and retrieve the results
* control data entities as a response to the request from a remote entity

### Use Cases

#### Link FDM I

When a fault occurs on the link, e.g. between TE and AN, and affects communication capability, each of the controllers may detect the fault and generate alarm from its own perspective.

In order to ease fault isolation and recovery, it is necessary to notify locally provided information to a remote entity for aggregation to the network entity with more resources.

In order to detect faults, the controllers shall be able to monitor each of the ports as well as the medium. As the access network is decomposed into a NA and BH, ANC should accomplish such task via either entity observing the links towards both TE and AR, as well as the one between NA and BH.

By using FDM functions, network entity may also be able to diagnose the cause of the problem and take corresponding countermeasure actions for recovery depending on the relevant information and resources it has.

For some faults there is no need for any short term action, since the fault condition will only last for a short period of time and then disappear.

Figure 7-8-2 illustrates the deployment of link FDM that can diagnose link failures in local area network, access network, and link between BH and AR, respectively.



1. In local area network



1. In access network



1. Between link from BH to AR

Figure 7-8-2: Link FDM I

#### Link FDM II

A mobile TE may seek services from multiple NA controlled by the same controller.

As these NAs usually operating in overlapping area. It allows ANC to do enhanced features, such as interference coordination, load balancing, mobility support, etc.

Thus, it is necessary for ANC to monitor multiple communication interfaces simultaneously and control multiple NAs in a coordinated fashion.

For some faults, additional means, such as test and diagnostic process may be necessary in order to obtain the required level of detail, e.g. an 802.11 AP requests specific station to perform scanning process, in either passive or active way, and convey the information.

As shown in Figure 7-8-3, one NA provides the initial testing (e.g., 802.11 passive scan) report to the ANC indicating that a neighboring NA is using the same wireless channel. The ANC will take some action, e.g. change channel assignment to the other NA, to mitigate mutual interference.



Figure 7-8-3: Link FDM II

#### Path FDM

As the [backhaul network infrastructure](http://www.exfo.com/library/sales-marketing-resources/marketing-documents/bu2-bu5-mobile-backhaul-network-assessment-brochure) evolves, it is necessary to provide operators as well as service providers a comprehensive and scalable testing and monitoring solution to gain real-time, end-to-end insight into service performance.

In IEEE 802 access networks, an integrated model of BH may consist of multiple IEEE 802.1 bridges, each with restricted management access to other’s equipment. As increasing number of bridges are used as BH, to perform a full scale of link FDM functions will exhaust the resources in ANC.

The purpose of path FDM is to detect and isolate the connectivity fault with a domain which denotes a segment of path bounded by end points.

These configured end points issue trains of point-to-point messages and multicast messages to determine the availability of the path.

Figure 7-8-4 depicts using path FDM in mobile backhaul service monitoring.



Figure 7-8-4: Path FDM

### Functional Requirements

In order to minimize the effects of faults on the QoS as perceived by the network users, FDM functions are necessary to support:

* Process for discovery of a remote entity’s FDM capability should be supported.
* The parameters, the thresholds, as well as the process flows and restoration actions depending on the nature and severity of the faults should be configurable.
* Notify FDM information, including alarms, to a remote entity should be supported.
* The functions of detecting faults in the network affecting the hardware, the software, the communication and the end-to-end connectivity should be supported.
* The functions to determine the cause of the failure should be supported.
* The functions to isolate the faulty resource or to recover from failures should be supported.

### FDM specific attributes

#### Terminal

* Self-check parameters
	+ E.g. communication interface status, device internal status, etc.
* R1 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R8 alarm
	+ E.g. communication alarm

#### Node of Attachment

* R1/R6 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R5 FDM information
	+ E.g. R1/R6 link monitoring results, testing results, etc.

#### Access Network Controller

* Self-check parameters
	+ E.g. communication interface status, device internal status, etc.
* R5/R7 configuration parameters
	+ E.g. remote test command, NA/BH configuration command, etc.
* R8/R9 alarm
	+ E.g. communication alarm

#### Backhaul

* R6/R3 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R7 FDM information
	+ E.g. R6/R3 link monitoring results, testing results, etc.

#### Access Router

* Self-check parameters
	+ E.g. communication interface status, device internal status, etc.
* R3 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R9 FDM configuration parameters
	+ E.g. remote test command, etc.
* Alarm
	+ E.g. QoS alarm

### FDM specific basic functions

#### Capability discovery

FDM provides a mechanism to detect the presence of FDM functionalities at the remote entity. The discovery procedure identifies the devices in the network along with their FDM capabilities, such as supported functions and configured parameters and thresholds.

For specific network entity, supported FDM functions and the implementation of these functions depend on the HW and SW resource it has, rather than on the its role in a network session.

It typically involves the discovery of a TE by AN. It may also involve discovery of two connected entities between the NA and the backhaul, inside the backhaul, or between the backhaul and the AR.

The controller should be able to response with the local FDM capability, when a FDM capability request is received from a remote controller. If necessary, it may announce its FDM capability to the remote controllers actively.

#### Remote failure indication

Remote failure indication is provided to a remote entity that either software, hardware or transmitter and receiver of local entity is nonoperational.

In order to detect fault, the controllers may use autonomous self-check circuits and daemon programs to validate the availability of hardware and software. As a result of detection, appropriate alarm should be generated by the faulty entity which contains all the information provided by the fault detection process.

For some faults there is no need for any short term action, since the fault condition lasted for a short period of time only and then disappeared.

The alarms can be stored, and forwarded to a remote entity in the form of unsolicited notification. If forwarding is not possible at this time, e.g. due to communication breakdown, the notification shall be sent as soon as the communication capability has been restored.

All alarms generated may be filtered and input into a list within local entity, which could be provided to a remote entity when requested.

Some physical layer devices have specific remote failure signaling mechanisms in the physical layer. The definition of specific remote failures depends on the different 802 technologies.

#### Link monitoring

The link monitoring is a mechanism to monitor the performance of the communication interface, the operation of communication protocols, such as miscellaneous events and status codes during the network setup phase, as well as the medium. Measurement procedures are provided on the physical or logical resources to evaluate of the quality of services.

It also provides the mechanism necessary to exchange the monitored information about link between entities, or notify to a remote entity.

Link monitoring may supply the following information for further FDM procedures:

* Communication statistic, such as counters of frame errors, counters of duplicate frames, round trip time, etc.
* Radio resource measurement, such as signal-to-noise ratio (SNR), signal-to-interference-noise ratio (SINR).
* Variables in the local Management Information Base (MIB).
* Configurations of the physical port
* The log of miscellaneous events and status codes during network setup phase

The majority of above information can be associated with thresholds for the declaration of fault occurrence and clearing conditions. When crossing a threshold or an error code is monitored, an alarm will be generated and notified to a remote entity. All alarms generated may be filtered and input into a list within local entity, which could be provided to a remote entity when requested.

#### Remote test

The remote test is the mechanisms provided to actively recognize the performance of the links or the validity of the remote entities. The testing procedures as such specified by IEEE Std 802.3, IEEE Std 802.11, IEEE Std 802.1Q and other IEEE standards are summarized as follows.

* Loopback test. This type of test involves a source sends out information and the remote entity echoes back some information to the source. There is a link-level loopback test when in loopback mode, all data received should be echoed back to the transmitter. It can be used for fault localization and link performance testing. Statistics from both the local and remote entity can be queried and compared at any time while the remote entity is in loopback mode. There is also a path-level loopback. This Ethernet ping scheme (unicast bi-directional request/response) can detect and verify connectivity failures along the path. Timestamps embedded in this ping message can be used to measure round-trip delay and one-way jitter.
* The local entity asks the remote entity to do some functionality test. The purpose is to verify that the remote entity is capable of some certain operation or its configuration meets the requirement. This type of tests include Association/Authentication Diagnostic where NA directs a TE to complete association/802.1X authentication process with a designated NA.
* Multicast test message that travels one or more hops to do path discovery or path connectivity check. For example, as one of the path FDM protocols, Continuity Check is a multicast unidirectional heartbeat message that can be used to detect connectivity fault anywhere between TE and AR based on the maintenance points’ configuration. The Continuity Check Message can also carry Remote Defect Indication and information about the status of the Bridge Port and/or aggregated port on which the transmitting MEP is configured. Linktrace, a.k.a. Ethernet Traceroute, is another example. The entity that is configured as MEP can transmit a multicast message in order to discover all the maintenance points and path for example from the TE through access network to AR. Each maintenance point along the path and the terminating point return a unicast Linktrace Reply to originating point. The Lintrace message flow between one end point (NA) to the other end point (AR) and intermediate points is shown in Figure 7-8-5.



Figure 7-8-5: Linktrace message flow

#### Aggregation

In order to ease fault isolation and recovery, it is necessary to configure the controller which has sufficient resources to aggregate information which is separately provided by multiple network entities or physical ports.

The information includes those associated with individual FDM function, such as remote failure indication, link monitoring and remote test, if necessary, also includes those provided by other functions which allows the aggregator have a comprehensive view of the overall health status of the network.

For instance, aggregation allows AR to retrieve alarms generated by TE via AN.

#### Failure Isolation

Failure isolation is to pinpoint one or more root causes of the faults, and helps to take correct actions to recover from the failure condition. The implementation of isolation algorithm and procedure can be tailored to the information provided according to the entity’s capability and FDM configuration.

If necessary, the determined and identified causes can be provided to a remote entity to help isolate the correlated alarms or to be used as a past experience.

#### Fault recovery

After a fault has been detected and the root cause have been identified, some actions and procedures are necessary in order to perform system recovery and/or restoration. Fault recovery provides such mechanism to get the system out of the failure state.

The recovery actions depend on the nature and severity of the faults, on the hardware and software capabilities of the entity and on the current configuration of the entity. The corresponding alarm shall be cleared, as soon as the system is confirmed of recovery.

The common recovery process is to enable the redundant resource, replacing the failed parts. Initiating the Spanning Tree Protocols to discover an alternate path will help to recover from the connectivity fault.

If there is no proper recovery countermeasures determined, the fault part of the system has to be isolated to limit the failure effects.

### Detailed procedures

#### Remote failure indication

To enable the remote failure indication, the local control entity (Ctrl 1) keeps monitoring the internal working state of the hardware and software. If a failure state is detected for any hardware or software resource, the remote control entity (Ctrl 2) is notified with the failure information. The procedure happens as follows:

* self-check circuits or daemon programs detect a failure state, an alarm is generated. The alarm is carried by an Alarm Report, and is sent out through the control reference port connecting the remote control entity;
* remote control entity receives the Alarm Report, the alarm information can be further utilized by aggregation or isolation.



Figure 7-8-6 Remote Failure Indication Procedure

#### Link monitoring

The Link monitoring procedure continues storing and maintaining the link monitoring information supplied by the data entity.

For the purpose of link monitoring, the control entities can interact and retrieve the link monitoring information with a remote control entity. The interaction procedure is described as follows:

* A control entity (Ctrl 2) generates Link Monitoring Request when necessary, and sends it out through the control reference port;
* Upon receiving the Link Monitoring Request, the remote control entity (Ctrl 1) can send a Link Monitoring Ack to acknowledge the reception, and then prepares the required monitoring information:
	+ the required information can be the up-to-date communication statistics and radio resource measurement results, the variables in MIB, the configurations of the physical port or the FDM event Log, which is prepared immediately;
	+ the required information can also be the communication statistics or the radio resource measurement, which needs to be prepared upon request. The monitoring process takes the action to count or measure for some period of time, according to the requirements in the Link Monitor Request
* The remote control entity generates Link Monitoring Report with the prepared information included, and sends it back to the original control entity. Link Monitoring Reply can be one time, or periodically repeated, according to the indication in Link Monitoring Request.



Figure 7-8-7 Link Monitoring Procedure

#### Remote test

The basic remote test procedure is shown in Figure 7-8-8. Local controller (Ctrl 2) sends a Remote Test Request to a remote controller (Ctrl 1). The remote controller responds with a Remote Test Ack if it has the corresponding FDM capability. Then the remote test process begins. After the test process ends, Ctrl 1 replies to Ctrl 2 with the Remote Test Report.



Figure 7-8-8: Remote test procedure

#### Aggregation

Referring to Figure 7-8-9, the procedure of local control entity retrieving FDM information from a remote entity is stated as below:

* Local control entity (Ctrl 2) initiates an Aggregation Request to a remote control entity (Ctrl 1) to retrieve necessary FDM information.
* Upon receiving the Aggregation Request, the remote control entity processes the aggregation according to the indication within the Aggregation Request.
	+ The aggregation process may involve FDM information from multiple remote entities that connected to the aggregator. This FDM information is provided individual FDM basic functions.
* The remote control entity generates an Aggregation Report with aggregated information included, and sends it back to the initiator through the control reference port.
* The initiator receives the Aggregation Reply. The aggregated FDM information can be used for further aggregation or fault isolation.



Figure 7-8-9 Aggregation Procedure

### Mapping to IEEE 802 Technologies

#### Overview

The following table provides IEEE 802 technology specific attributes for the fault diagnostics and maintenance (FDM).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 802.3 | 802.11 | 802.16 | 802.22 |
| R1/R6/R3 link monitoring parameters | Errored Symbol Period, Errored Frame, Errored Frame Period, Errored Frame Seconds Summary | RSSI, LQ, retry count, radio measurement (Channel Load, Noise Histogram, etc.), link measurement (RCPI, RSNI, etc.), neighbor report (AP reachability, capabilities, etc.) | Channel measurement (RSSI, CINR, coexistence neighbor report), CSI monitoring report, etc. |  |
| R8 alarm | Link fault, dying gasp, critical event | Status code | Error code |  |
| R5/R7/R9 configuration parameters | Loopback mode configuration. | Association/authentication test, switch channel, change TX power |  |  |

#### IEEE 802.3 specifics

#### IEEE 802.11 specifics

#### IEEE 802.16 specifics

#### IEEE 802.22 specifics