|  |
| --- |
| Fault Diagnostics and Maintenance Functional Description |
| Date: 2016-05-23 |
| **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 3

7.8.3 Use Cases 4

7.8.3.1 NMS receives alarm notification 4

7.8.3.2 NMS sends request to ANC 4

7.8.3.3 Fault isolation by ANC 5

7.8.4 Functional Requirements 6

7.8.5 FDM specific attributes 6

7.8.5.1 Terminal 6

7.8.5.2 Node of Attachment 6

7.8.5.3 Access Network Controller 6

7.8.5.4 Backhaul 6

7.8.5.5 Access Router 7

7.8.6 FDM specific basic functions 7

7.8.6.1 Capability discovery 7

7.8.6.2 FDM registration and configuration 7

7.8.6.3 Remote failure indication 7

7.8.6.4 Link monitoring 8

7.8.6.5 Testing 8

7.8.6.6 Aggregation 9

7.8.6.7 Fault isolation 10

7.8.6.8 Fault recovery 10

7.8.7 Detailed procedures 10

7.8.7.1 Remote failure indication 10

7.8.7.2 Link monitoring 11

7.8.7.3 Testing 12

7.8.7.4 Aggregation 13

7.8.8 Mapping to IEEE 802 Technologies 13

7.8.8.1 Overview 13

7.8.8.2 IEEE 802.3 specifics 13

7.8.8.3 IEEE 802.11 specifics 13

7.8.8.4 IEEE 802.16 specifics 14

7.8.8.5 IEEE 802.22 specifics 14

# Functional Decomposition and Design

## Fault Diagnostics and Maintenance (FDM)

### Introduction

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 element (NE), cause the malfunction of the logical and physical resources and will, in severe cases, lead to the complete unavailability of the respective NE. A fault may also occur on a link and cause communication performance deterioration, connectivity loss etc., thus affect quality of service.

For example, fault instance in a wireless local network scenario typically appears as the problem of a hardware or software failure of AP and station that establish communication; the problem of a setup mistake; the problem of the overloaded channel; and the problem caused by radio propagation.

As a consequence of faults, the appropriate alarms related to the physical or logical resources affected by the faults, shall be generated by the faulty NE. Such alarms shall contain all the information provided by the fault detection process.

Fault diagnostics and maintenance (FDM) provide 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.

FDM includes protocols defined by IEEE 802 provided as FDM tools across network interfaces and relative management agents that resides in each control entity. Examples of such FDM tools include 802.3ah, 802.1ag for Ethernet links, and 802.11k, v for wireless links.

### Roles and identifiers

In a real deployment, network management service (NMS) and ANC plays an important role in configuring FDM functionality across multiple devices in the network, and for automating the monitoring and troubleshooting of network faults. Such FDM functions and operator interfaces can mimic the actions of an expert and carry out troubleshooting steps faster, hence minimizing service downtime.

The NMS is mainly supported by ANC but it may also involve direct access to other network element. Since NMS is in the operator domain, the requirement and its detailed function blocks are out of scope of this document.

To provide to the NMS the fault management capability for the network implies that the ANC needs to provide information about failures, configuration of parameters, root cause from diagnostics and results of recovery and testing. As a central controller in access network, ANC provides the foundation for operators and service providers to manage access networks in an efficient manner. It allows the NMS to operate the FDM information within the subordinate entities and achieve management interoperability among multi-vendor equipments. It contains functions to manage NEs directly and provides support to the applications in the OSS (Operation Support System) through NMS.

R11 represent the management interfaces between NMS and the access network controller so as to connect system of any vendor to the NMS.

In order to detect faults, each network element like TE, NA, BH, and AR may use autonomous self-check circuits and measurement procedures to observe the performance of physical ports. The FDM agent within each NE is usually developed by equipment vendors to carry out FDM basic operations and provide functional support to ANC.

Control interfaces, i.e. R5, R7, R8, R9, are used to exchange necessary FDM information for basic functions, e.g.

* configure the parameters, thresholds and FDM process
* notify the alarms of detected fault and result of recovery to ANC
* aggregate fault related information, such as communication statistics from subordinate NE
* control specific NE to enter test mode to execute the testing procedure and retrieve test results

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

### Use Cases

This section describes some FDM use cases that are used in deployment. These use cases are not meant to be exhaustive.

#### NMS receives alarm notification

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 for TE or NA to notify local information to ANC for aggregation.

By using FDM functions, ANC may 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. However for some faults ANC may not be able to diagnose the root cause then it notifies NMS about the details of the aggregated information related to the fault.

In some cases, NMS may get alarm notifications from ANCs provided by multiple vendors. NMS can do fault isolation either automatically or by human interaction utilizing expert knowledge.

#### NMS sends request to ANC

NMS may send request to ANC for several purposes, for example,

* NMS can access TE and AR through the interface to ANC and request for configuration.
* NMS can request the configuration and capability profiles from the ANC.
* NMS can retrieve aggregated information from ANC about NE alarms, events or statistics.
* NMS can initiate remote test, e.g. requiring ANC to schedule loopback test (Ethernet ping) to help pin pointing the fault location.

When root cause has been identified, NMS can request ANC to do failure recovery. The process of fault recovery can be initiated manually by the operator through NMS.

For instance, NMS can initiate recovery actions if the operator deems that NE is not able to perform its functions as the result of analysis and correlation of alarm reports and performance data, or if the operator wants to verify the newly replaced or repaired unit can provide the intended service.

#### Fault isolation by ANC

In a lot of scenarios ANC can do failure isolation and failure recovery on its own. When the root cause and effect of the fault are identified, ANC may autonomously take fault recovery actions in order to minimize the service degradation or disruption.

For some faults, additional means under the control of ANC, such as test and diagnostic process may be necessary in order to obtain the required level of details. For example, an 802.11 AP requests a specific station to perform scanning process, in either passive or active way, then feedback the information.

In the following scenario, a mobile TE may seek services from multiple NAs controlled by the same controller. As these NAs usually operating in overlapping area, the ANC is allowed 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.

As shown in Figure 7-8-1, 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 actions, e.g. change channel assignment to the other NA, to mitigate mutual interference.



Figure 7-8-1: Multiple NAs controlled by the same controller

### Functional Requirements

* Process for discovery of a remote entity’s FDM capability should be supported.
* The parameters, thresholds, as well as the process flows and restoration actions depending on the nature and severity of the faults should be configurable.
* Notifying FDM information, such as alarms, counters, thresholds, events, MIB variables, status codes, discovery, system logs, etc. to a remote entity should be supported.
* The functions of detecting faults in the network affecting the hardware, the software, the communication interfaces should be supported.
* The functions to determine the root 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

* Self-check parameters
	+ E.g. communication interface status, device internal status, etc.
* R1/R6 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R5 alarm
	+ E.g. communication alarm

#### Access Network Controller

* R5/R7/R8/R9 configuration parameters
	+ E.g. remote test command, NA/BH configuration command, etc.
* R5/R7/R8/R9 alarm
	+ E.g. communication alarm
* R11 network management information
	+ E.g. aggregated alarm/event, etc.

#### Backhaul

* Self-check parameters
	+ E.g. communication interface status, device internal status, etc.
* R6/R3 link monitoring parameters
	+ E.g. measurements, counters, thresholds, etc.
* R7 alarm
	+ E.g. communication alarm

#### 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 alarm
	+ E.g. QoS alarm

### FDM specific basic functions

#### Capability discovery

The discovery procedure identifies the devices in the network along with their FDM capabilities, such as supported functions and configurable parameters and thresholds.

The procedure typically involves the discovery of a TE by NA. It may also involve discovery of any directly connected NEs using protocols defined by IEEE 802.

Local NE should be able to respond with its FDM capability, when the FDM capability request is received from a remote NE. If necessary, it may notify local FDM capability to the remote NE actively.

The FDM capability of each NE should be forwarded to ANC to enable relevant FDM functions, then the information can be accessed manually by operator through NMS.

#### FDM registration and configuration

FDM registration enables NMS to register to receive alarms and other FDM information from ANC. NMS sends registration request to ANC in order for operator to access the FDM information conveyed by ANC.

NMS may initiate configuration request to ANC after registration. Upon receiving a request, ANC sets parameters related to supported FDM functions at NE, such as thresholds, alarm severities, alarm filtering criteria etc.

ANC should send a confirmation to NMS to indicate whether the requested registration or configuration operation has been implemented successfully.

#### Remote failure indication

Remote failure indication is provided to notify a remote NE that either software, hardware or communication interface of local entity is nonoperational.

The NEs may use autonomous self-check circuits and daemon programs to validate the availability of hardware and software. A failure event of the hardware or software should be reported to a remote NE. For instance, when an unrecoverable local failure condition has occurred like a device power down, a dying gasp event can be notified to a remote NE. The definition of specific remote failures depends on the different 802 technologies.

NE may be able to generate the alarm based on the failure event and relevant information provided by the detection process. The alarms should be forwarded to ANC in the form of unsolicited notification as soon as possible if they are not suppressed by individual NE, where they are stored, retained, cleared and accessed manually by operator through NMS. 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.

#### Link monitoring

Link monitoring is a mechanism to monitor the performance of the communication and the implementation of protocols during network setup and network operation.

Link monitoring is accomplished by NE using measurements on physical or logical resources and administered by ANC that permits the inclusion of diagnostic information. As KPI for evaluating the quality of services (QoS) and quality of experiences (QoE), the information provided may also include counters, thresholds, events, MIB variables, status codes, discoveries, system logs, etc.

Link monitoring should supply the following information for further FDM processing:

* Communication statistics in a specified window, e.g. round trip time, count of error frames, duplicate frames, retransmissions, etc.
* Radio resource measurement, e.g. RSSI, LQI, signal-to-interference-noise ratio (SINR)
* Events and status code during network entry, re-entry and secession
* Variables in the local Management Information Base (MIB)
* Neighbor information and topology provided by a channel scan or discovery protocols, e.g. LLDP
* System logs
* Threshold crossing event when well-defined thresholds are specified by ANC.

Within each NE, all information acquired by the mechanism shall be put into a set for temporary storage. The NEs shall be able to provide such information set to the ANC when requested, then from the ANC the information can be manually accessed by operator through NMS.

When threshold is configured for an entity by the ANC, an alarm may be generated based on the threshold crossing events. It should be forwarded to ANC as soon as possible if they are not suppressed by individual NE.

#### Testing

Testing can be used in different phases of the FDM to assist fault mitigation. For example:

* when a fault has been detected and if the information provided through the alarm report is not sufficient to localize the faulty resource, tests can be executed to better localize the fault;
* during normal operation of the NE, periodic tests can be executed to support proactive maintenance;
* once a faulty unit has been repaired or replaced, before it is restored to service, tests can be executed to verify the its working condition.

Besides the self-check on the hardware and software of the unit, remote test is a mechanism provided to actively recognize the performance of the links or the validity of the remote NEs. The testing procedures as 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 tests involve a local NE sending out information and the remote NE echoing back some information to the source. When the loopback test is carried out on the direct link, all data received should be echoed back to the transmitter. When it is carried out across multiple links, unicast bi-directional request and response messages are implemented as the Ethernet ping scheme. Timestamps embedded in this ping message can be used to measure round-trip delay and one-way jitter.
* Continuity Check test. The multicast unidirectional heartbeat message is used to detect connectivity fault anywhere between TE and AR based on the configuration of the maintenance points along the path.
* Linktrace test, a.k.a. Ethernet Traceroute. Initial NE 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 returns a unicast Linktrace Reply to originating point.

Regardless of the context where the testing is used, its target is always the same: verify if a system’s physical or functional resource performs properly and, in case it happens to be faulty, provide all the information to help the operator localize and correct the faults.

Testing can be initiated by ANC or by the operator through NMS.

#### Aggregation

In order to ease fault isolation and recovery, it is necessary for ANC which has sufficient resources to aggregate FDM information which is separately provided by multiple NEs before it is notified to the NMS.

Typically, the information includes the unsuppressed alarms which are forwarded to ANC and stored as a list of active alarms. It also includes those associated with individual FDM functions, such as link monitoring and testing, which allow the ANC have a comprehensive view of the overall health status of the network.

As a single fault may result in the generation of multiple alarms and events and may spread over a wide geographical area from affected entities over time, alarms captured in the active alarm list may be correlated to each other. If possible, the alarms are partitioned into sets where the alarms within one correlated set have a high probability of being caused by the same fault. A correlated set may also contain events and other FDM information that are considered to be related with the fault, which are actively retrieved by ANC.

The aggregation enables NMS to retrieve the active alarms as well as other FDM information. Filters may be applied when accessing the information in aggregation, e.g. TE ID as the filtering criteria. Aggregation can forward information or the correlation set to failure isolation function to find the root cause of the fault.

#### Fault isolation

Fault isolation is to pinpoint one or more root causes of the faults, and help take correct actions to recover from the failure condition.

The implementation of isolation algorithm and procedure can be tailored based on the following (for example):

* the information and correlation set provided by aggregation
* the ANC’s capability and configuration
* operators’ network management experience

When the root cause and effect of the fault are identified, ANC may autonomously take fault recovery actions in order to minimize the service degradation or disruption.

If the root cause of the fault cannot be provided, the alarms and correlated information will be forwarded to NMS for further analysis.

#### Fault recovery

After a fault has been detected and the root cause has 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, the hardware and software capabilities of the NE and the current configuration of the NE. For the faulty single NE, ANC may request NE to enable the redundant resource, replace the failed parts, reset the hardware, or initialize the software. For the sub-network with connectivity fault, ANC may initiate the Spanning Tree Protocols to discover an alternate path.

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

Fault recovery can be manually initiated by operator through NMS. In this case, NMS sends a request to ANC to execute the specified fault recovery action.

The corresponding alarm shall be cleared, as soon as the system recovery is confirmed.

### Detailed procedures

#### Remote failure indication

To enable the function of remote failure indication, the unsuppressed alarm can be reported to ANC, directly or through another NE.

1. NE may detect the fault and generate an appropriate alarm report forwarding to ANC through control interfaces. The procedure involving TE and ANC is shown in Fig. 7-8-2(a).
2. In the other case, the failure event may be sent to a remote NE through data interfaces following IEEE 802 protocols. On the remote NE, incoming events will be identified then trigger the generation of alarm. To be more specific, Fig. 7-8-2(b) shows the procedure involving TE, NA and ANC.
3. The alarm report may associate with a series of failure events from one or multiple NEs. In addition, it may also carry the following information:
* The type of the fault (e.g. communication, quality of service, processing error, equipment, environmental)
* The severity of the fault (e.g. cleared, indeterminate, critical, major, minor, warning)
* The time when the fault was detected
* The probable cause of the fault (e.g. transmit failure, receive failure, threshold crossed)
* The units at fault. For the hardware faults, it indicates the smallest replaceable unit at fault. For the software faults: the faulty software component (e.g. corrupted files or software codes).



Figure 7-8-2 Procedure of Remote Failure Indication

#### Link monitoring

Link monitoring is always initiated by ANC or manually by the operator through NMS.

1. ANC sends the link monitoring request to NE via the control interface to initiate the monitoring process. The request may carry the following information:
	* transaction ID
	* type
	* parameters (e.g. the measurement frequency, duration of measurement at each time)
	* report condition
	* report interval
	* granularity interval
2. Upon receiving the request, NE will execute the monitoring process that may involve a second NE. As shown in Fig. 7-8-3, NE1 needs to send an additional measurement request to NE2 via data interface and retrieves the results from the remote entity.
3. When report condition is met, NE should send link monitoring report to ANC which may carry the following information:
	* transaction ID
	* type
	* time stamp
	* link monitoring data

The monitoring report can be sent for one time, conditionally or periodically as indicated by the request. If it is indicated as a condition report, the relevant threshold should be included in the link monitoring request. The threshold crossing report may trigger the generation of alarm to be forwarded to ANC.



Figure 7-8-3 Procedure of link monitoring

#### Testing

Testing procedure can be initiated by ANC or manually by the operator through NMS. In the first case,

1. ANC sends request to NE to initiate the testing procedure. The request may carry the following information,
	* NE ID
	* Testing command
	* Testing parameters
2. The NE executes the test and return the test results to ANC



Figure 7-8-4: Procedure of ANC initiated testing

#### Aggregation

As shown in Figure 7-8-6, NMS sends an aggregation request to the ANC including the following information:

* Filtering criteria, e.g. TE ID
* Period of the response message
* List of attributes to specify the requirements for the ANC

When the ANC receives the aggregation request, it should send an aggregation response immediately to the NMS with the following information:

* ANC ID
* List of FDM information as specified

The ANC will periodically respond the above information to the NMS at the specified interval until the termination by the NMS.



Figure 7-8-6 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### IEEE 802.3 specifics

#### IEEE 802.11 specifics

#### IEEE 802.16 specifics

#### IEEE 802.22 specifics