|  |
| --- |
| Fault Diagnostics and Maintenance Functional Description |
| Date: 2016-05-26 |
| **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

7.8.2.1 Network Management System 3

7.8.2.2 Element Management System 3

7.8.3 Use Cases 4

7.8.3.1 Alarm notification to NMS 4

7.8.3.2 NMS requests to ANC 4

7.8.3.3 Automatic fault recovery by ANC 5

7.8.4 Functional Requirements 5

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 6

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 Fault isolation 7

7.8.6.4 Fault recovery 7

7.8.7 Detailed procedures 8

7.8.7.1 Remote failure indication 8

7.8.7.2 Link monitoring 9

7.8.7.3 Testing 10

7.8.7.4 Management information aggregation 11

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 13

7.8.8.5 IEEE 802.22 specifics 13

# 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 or the loss of redundancy in case of a redundant configuration. A fault may occur on an NE, cause the malfunction of the logical and physical resources and will, in severe cases, lead to the complete unavailability of the faulty 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 area network scenario typically appears as the problem of a hardware or software failure of NA and TE that established 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 capable 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 access network operator to monitor the health of the network and quickly determine failing link location and/or fault condition, 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 reside in each NE. 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 element manager (EM) in ANC play an important role for configuring FDM functionality across multiple elements in the network, and for automating the monitoring and troubleshooting the network faults. Such FDM functions can mimic the actions of an expert and carry out troubleshooting steps faster, hence minimizing service downtime.

#### Network Management Service

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

R11 represents the management interfaces between NMS and the EM in ANC so as to connect system of any vendor to the NMS.

#### Element Manager

To provide to the NMS the fault management capability for the network implies that the EM in 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 the access network, the ANC containing multiple EMs provides the foundation for network operators to manage access networks in an efficient manner. It allows the NMS to operate the FDM information within the subordinate elements and achieve management interoperability among multi-vendors. It contains functions to manage NEs directly and provides support to the applications in the OSS through NMS.

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

* configuration of the parameters, thresholds and FDM process,
* notification of the alarms of fault and result of recovery,
* various fault management information for aggregation,
* testing request for specific NE and testing results.

In order to detect faults, network element such as TE, NA, BH, and AR may use autonomous self-check to monitor internal status and measurement procedures to observe the performance of physical ports. The FDM agents within each NE which carry out basic FDM operations and provide functional support to the EM in ANC are usually vendor specific.

Data interfaces, i.e. R1, R6, and R3 are used to carry test requests and results in order to provide additional information.

### Use Cases

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

#### Alarm notification to NMS

When a fault occurs on the link, e.g. between TE and AN, and affects communication capability, both NEs may detect the fault and generate alarm from its own perspective. In order to ease fault isolation and recovery, it is necessary for TE and NA to notify local information to ANC for aggregation.

By using FDM functions, ANC may be able to diagnose the cause of the fault and take corresponding countermeasure actions for recovery. In the case that ANC is not able to diagnose the root cause, it notifies NMS about the relevant aggregated information.

NMS may get alarm notifications from EMs in ANC provided by multiple vendors. NMS can do fault isolation by human interaction utilizing expert knowledge.

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.

#### NMS requests to ANC

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

* NMS requests for configuring the subordinate elements through ANC,
* NMS requests for polling configuration and capability profiles of the subordinate elements through ANC,
* NMS requests for polling aggregated information from ANC about the specified NE,
* NMS requests for initiating tests, e.g. requiring ANC to schedule loopback test (Ethernet ping) to pinpoint the fault location,
* NMS requests ANC to initiate fault recovery when root cause has been identified. The fault recovery process may include replacement of a malfunction NE and repair of the faulty unit, etc.

#### Automatic fault recovery by ANC

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

For some faults, additional tests and diagnostics under the control of ANC may be necessary in order to obtain the required level of details.

In a scenario that multiple NAs operate in overlapping area, a mobile TE may seek services from the NAs controlled by the same controller. In this case, the ANC is allowed to do enhanced features, such as interference coordination, load balancing, mobility support, etc. It may be necessary for ANC to monitor multiple communication interfaces simultaneously and perform the FDM functionalities in a coordinated fashion.

As shown in Figure 7-8-1, one NA is requested to provide the diagnostic (e.g. 802.11 passive scan) report for the ANC to verify whether a neighboring NA operating on the same wireless channel causes severe mutual interference. The ANC automatically initiates the recovery actions, e.g. re-assign channels, to mitigate the interference.



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

### Functional Requirements

* Automatic discovery of FDM capabilities of remote entities should be supported.
* The parameters, thresholds, as well as the process flows and actions should be configurable.
* Notifying and polling from a remote entity about FDM information, such as alarms, counters, thresholds, events, MIB variables, status codes, discovery, system logs, etc, should be supported.
* The functions to detect faults that affect hardware, software, and communication performance should be supported.
* The functions to determine the root cause of the fault should be supported.
* The functions to isolate or replace the faulty resource for recovery should be supported.

### FDM specific attributes

#### Terminal

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

#### Access Network Controller

* R5/R7/R8/R9 configuration parameters
	+ E.g. testing command, configuration request, etc.
* R5/R7/R8/R9 alarm
	+ E.g. communication alarm
* R11 network management information
	+ E.g. aggregated alarms, events, etc.

#### Backhaul

* Self-check parameters
	+ E.g. communication interface status, 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, 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 to a remote NE, when receiving discovery request. It should also be able to notify local FDM capability to the remote NE actively.

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

#### FDM registration and configuration

NMS should complete the registration process to enable its FDM functionality. By sending request to a specific ANC, NMS registers to receive alarms and other FDM information.

NMS may initiate configuration request to ANC after registration. Upon receiving the request, ANC will set the parameters at NE according to its FDM capability, 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.

#### 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 recovery actions in order to minimize the time of 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, countermeasure actions and procedures are necessary to recover the system and/or network. 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 single faulty NE, ANC may request to enable the redundant resource, to replace the faulty parts, to reset the hardware, or to re-initialize the software. For data path having 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 NE or sub-network 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

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

NE may use autonomous self-check circuits and daemon programs to validate the availability of hardware and software. As a result, failure event should be notified to a remote NE. For instance, a dying gasp event is notified to a remote NE indicating local power down failure has occurred. The definition of specific failures is implementation specific and depends on 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.

Detailed procedures of remote failure indication is defined as follows,

1. NE detects the fault and generates 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. Alternatively, the failure event may be firstly 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. Fig. 7-8-2(b) shows such procedure involving TE, NA and ANC.
3. The alarm report may associate with a series of failure events from one or multiple NEs. 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, 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 a mechanism to monitor the performance of the communication and the implementation of protocols for connection setup and connection operation.

Link monitoring is accomplished by NE with data interfaces using measurements on physical or logical resources and administered by ANC that permits the inclusion of diagnostic information. For evaluating the quality of services (QoS) and quality of experiences (QoE), the information provided as KPI may include counters, thresholds, events, MIB variables, status codes, discoveries, system logs, etc. Specifically, the following information can be supplied by NE to ANC for further FDM processing:

* Communication statistics in a specified time window, e.g. count of error frames, duplicate frames, retransmissions, channel busy ratio,
* Radio resource measurement, e.g. RSSI, LQI, signal-to-interference-noise ratio (SINR)
* Events and status code during network entry, network re-entry and disconnection
* Variables in the local Management Information Base (MIB)
* Neighbor information and topology provided by discovery protocols, e.g. LLDP
* Environmental information provided by e.g. 802.11 channel scan and diagnostics
* Records from system logs
* Threshold crossing event when well-defined thresholds are specified by ANC.

Within each NE, all information acquired by link monitoring shall be provided to EM in ANC when requested. And it can be manually accessed by operator through NMS.

The threshold crossing report may trigger the generation of alarm. It should be forwarded to ANC as soon as possible if they are not suppressed by individual NE.

Detailed procedures of link monitoring is defined as follows,

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 starts the monitoring process that may involve a second NE. As shown in Fig. 7-8-3, NE1 sends additional measurement request to NE2 via data interface in order to retrieve the results from the remote NE.
3. When report condition is met, NE1 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 to report conditionally, the relevant threshold should be included in the link monitoring request.



Figure 7-8-3 Procedure of link monitoring

#### 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 by the alarm report is not sufficient to localize the faulty resource, tests can be executed to better localize the fault;
* during connection operation, NE may periodically execute tests to support proactive maintenance;
* once a faulty unit has been repaired or replaced, before it is restored to service, tests may be executed to verify its working condition.

Besides the self-check test on the hardware and software, remote test is a mechanism provided to actively recognize the performance of the links or the availability of remote NEs. The descriptions of remote test specified by IEEE 802 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.

Testing procedure can be initiated by ANC or manually by the operator through NMS. The former is defined as follows,

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



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

#### Management information aggregation

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

Typically, FDM information includes the unsuppressed alarms which are forwarded to ANC and stored as a list of active alarms. It also includes the information associated with individual FDM functions, such as link monitoring and testing. Management information aggregation allows the ANC to 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. The alarms can be 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 information that are considered to be related with the fault.

Management information aggregation also enables NMS to retrieve the active alarms as well as other FDM information from ANC. As shown in Figure 7-8-6, NMS sends an aggregation request to ANC including:

* transaction ID
* filtering criteria, e.g. TE ID
* report interval
* 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:

* transaction ID
* list of FDM information as specified

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



Figure 7-8-6 Management Information Aggregation Procedure

As a result, the output of management information aggregation should be used for failure isolation to find the root cause of the fault.

### 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