Network Working Group N. Davis, Ed.
Internet-Draft Ciena
Intended status: Informational A. Farrel, Ed.
Expires: 29 May 2025 Old Dog Consulting
T. Graf
Swisscom
Q. Wu
Huawei
C. Yu
Huawei Technologies
25 November 2024

Some Key Terms for Network Fault and Problem Management
draft-ietf-nmop-terminology-08

Abstract

This document sets out some terms that are fundamental to a common understanding of network fault and problem management within the IETF.

The purpose of this document is to bring clarity to discussions and other work related to network fault and problem management, in particular to YANG models and management protocols that report, make visible, or manage network faults and problems.

Status of This Memo

Copyright Notice

described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Successful operation of large or busy networks depends on effective network management. Network management comprises a virtuous circle of network control, network observability, network analytics, network assurance, and back to network control. Network fault and problem management is an important aspect of network management and control solutions. It deals with the reporting, inspection, correlation, and management of events within the network. The intention is to focus on those events that have a negative effect on the network's ability to forward traffic in an optimal way. Fault and problem management extends to include actions taken to determine the causes of problems and to work toward recovery of optimal network behavior.

Commenté [MB1]: May be bring «Fault management encloses a set of functions to detect, isolate, notify, and correct faults encountered in a network as well as to maintain and examine error logs. » from rfc6632 as we don't have an entry for fault management.

Commenté [MB2]: Or «as intended/expected»

I see «expected behavior» is used in other parts of the doc.

A number of work efforts within the IETF seek to provide components of a fault management system, such as YANG models or management protocols. It is important that a common terminology is used so that there is a clear understanding of how the elements of the management and control solutions fit together, and how faults and problems will be handled.

This document sets out some terms that are fundamental to a common understanding of network fault and problem management. While "faults" and "problems" are concepts that apply at all levels of technology in the Internet, the scope of this document is restricted to the network layer and below, hence this document is specifically about "network fault and problem management."

~~The terms defined in this document are principally intended for consistent use within the IETF. Where similar concepts are described in other bodies, an attempt has been made to harmonize with those other descriptions, but there is care needed where terms are not used consistently between bodies or where terms are applied outside the network layer. If other bodies find the terminology defined in this document useful, they are free to use it.~~

Note that some useful terms are defined in [RFC3877] and [RFC8632]. The definitions in this document are informed by those documents, but they are not dependent on that prior work.

2. Usage of Terms

The terms defined in this document are principally intended for consistent use within the IETF. Where similar concepts are described in other bodies, an attempt has been made to harmonize with those other descriptions, but there is care needed where terms are not used consistently between bodies or where terms are applied outside the network layer. If other bodies find the terminology defined in this document useful, they are free to use it.

Other documents may make use of the terms as defined in this document. It is suggested here that such uses should use capitalization of the terms as in this document, and should include an early section listing the terms inherited from this document with a citation.

3. Terminology

This section contains key terms. It is split into three subsections~~.~~:

* Section 3.1 contains terms that help to set the context for the incident and fault management systems.

* Section 3.2 includes specific and detailed core terms that will be used in other documents that describe elements of the fault management systems.

* Section 3.3 provides two further terms that may be helpful.

3.1. Context Terminology

This section includes some terminology that helps describe the context for the rest of this work. The terms may be viewed as a cascaded hierarchy with each subsequent term building on the previous. The definitions are deliberately kept relatively terse. Further documents may expand on these terms without loss of specificity. Such contextualization (if any) should be highlighted clearly in these documents.

Network Telemetry: This is defined in [RFC9232] and describes the process of collecting operational network data categorized into network planes. Data collected through the Network Telemetry process does not contain network or device configuration information. Nor does it contain any data related to service definitions (i.e., “intent” per Section 3.1 of [RFC9315]).

Network Monitoring: This is the process of keeping a continuous record of a resource, function, or connectivity service. The term 'monitoring' focuses on one single dimension and measurement in dimensional data modeling [DimensionalModeling]. This could be a measurement of the service state, a network function measurement, or the state of a network function of a resource as an example.

Network Analytics: Network Analytics is the process of deriving analytical insights into or from operational network data. A

Commenté [MB3]: Unlike fault (which is mentioned) several times in the introduction, incident wasn’t mentioned before. I would some mentions earlier so that readers won’t have to guess why this is covered here.

Commenté [MB4]: Any reason why we are not consistent here vs previous bullet (vs mention of incident)?

Commenté [MB5]: Better to help readers find where to look.

process could be piece of software, a system, or a human that analyzes operational data and outputs new analytical data, ideally metadata (a symptom, for example), which is related to the operational data.

Network Observability: This is the enablement of network behavioral assessment through analysis of observed operational network data (logs, alarms, traces, etc.) with the aim of detecting symptoms of network behavior, and to identify, anomalies and their causes. Network Observability begins with information gathered using Network Monitoring tools and that may be further enriched with other operational data (e.g., change records). The expected outcome of the observability processes is identification and analysis of deviations in observed state versus the expected state of a network.

Thus, there is a cascaded sequence where:

* Network Telemetry: the process of collecting operational data from ~~the~~ a network.

* Network Monitoring: the process of creating/keeping a record of data gathered in Network Telemetry.

* Network Analytics: the process of deriving insights through the data recorded in Network Monitoring.

* Network Observability: the process of enabling behavioral assessment of ~~the~~ a network through Network Analytics.

3.2. Core Terms

The terms are presented below in an order that is intended to flow such that it is possible to gain understanding reading top to bottom. The figures and explanations in Section 4 may aid understanding the terms set out here.

System: An assembly of components that exhibits some behavior.

Resource: A component of a System.

Resource is a recursive concept so that a Resource may be a collection of other Resources (for example, a network node comprises a collection of interfaces).

Characteristic: Observable or measurable aspect or behavior associated with a Resource.

* A Characteristic may be considered with respect to the concept of dimensional modeling that is built on facts (see ~~'value'~~'Value', below) and dimensions (the contexts and descriptors that identify and give meaning to the facts).

* The term "Metric" is another word for "Characteristic".

Value: ~~A Value i~~Is the measurement of a Characteristic associated

Commenté [MB6]: Or a System?

Commenté [MB7]: For consistency.

Commenté [MB8]: Do you mean these are identical?

A characteristic can be characterized (sic) by one or multiple metrics, but don't think we can use them interchangeabily.

Commenté [MB9]: For consistency with other entries.

Commenté [MB10]: May be interpreted as a provided value is a measured one, while this can be used to set an objective (that will be used, e.g., to restrict the monitoring thresholds, etc.)

with a Resource. It may be in the form of a categorization (e.g., high or low), an integer (e.g., a count), ~~or~~ on a continuous variable (e.g., an analogue measurement), etc.

Commenté [MB11]: Other forms may considered.

a mis en forme : Français (France)

a mis en forme : Français (France)

Condition: ~~A Condition is a~~An interpretation of the Values of a set of Characteristics of ~~the~~ a Resource (with respect to working order or some other aspect relevant to the Resource purpose/ application).

Change: In the context of Network Monitoring, a Change is the variation in the Value of a Characteristic associated with a Resource.

* ~~Most~~ Not all Changes are ~~not~~ noteworthy (i.e., do not have Relevance).

* Perception of Change depends upon Detection, the sampling rate/accuracy/detail, and perspective.

Detect: To notice the presence of something (State, Change, activity, form, etc.).

Commenté [MB12]: occurrence?

* Hence also to notice a Change (from the perspective of the viewer).

Commenté [MB13]: That is? May be cite an example (monitor system and the like)

Event: The variation in Value of a Characteristic of a Resource at a measured instant in time (i.e., the period is negligible).

* Compared with a Change, which may be over a period of time, an Event happens at a measurable instant (e.g., measurement interval).

State: A particular Condition that something (e.g., a Resource) is in (at a specific time).

* While a State may be observed at a specific moment in time, it is actually achieved by summarizing the measurement over time in a process sometimes called State compression.

Commenté [MB14]: Do we have a doc to cite here?

Relevance: Consideration of an Event, State, or Value (through the application of policy, relative to a specific perspective, intent, and in relation to other Events, States, and Values) to determine whether it is of note to the system that controls or manages the network.

Commenté [MB15]: I agree with the use here as this reflects that this is not per «System» defined in the doc.

Occurrence: An Event with Relevance.

A particular Change with Relevance.

* An Occurrence may be an aggregation or abstraction of smaller Occurrences.

Commenté [MB16]: Finer-grain?

* Applies to all scales and scopes, i.e., is essentially fractal (can recurse indefinitely).

* Note that Occurrence is used here with respect to the temporal dimension.

Fault: An Occurrence that is not desired/required (as it may be indicative of a current or future undesired State). A Fault can generally be associated with a known cause. See [RFC8632] for a more detailed discussion of network faults.

Problem: A State regarded as undesirable and which may require remedial action. A Problem cannot necessarily be associated with a cause. The resolution of a Problem does not necessarily act on the thing that has the Problem.

* Note that there is a historic aspect to the concept of a Problem. The current State may be operational, but there could have been a failure that is unexplained, and the fact of that unexplained recent failure is a Problem.

* Note that whilst a Problem is unresolved it may continue to require attention. A record of resolved Problems may be maintained in a log.

* Note that there may be a State which is considered to be a Problem from several perspectives (e.g., a loss of light State may cause multiple services to fail). A State Change (so that the light recovers) may cause the Problem to be resolved from one perspective (the services are operational once more), but may leave the Problem as unresolved (because the loss of light has not been explained). There could be a further development (the reason for the temporary loss of light is traced to a microbend in the fiber that is repaired) resulting in that unresolved Problem now being resolved. But this leaves a further Problem still unresolved (why did the microbend occur in the first place?).

Commenté [MB17]: How this should interpreted? «e.g.» ?

Commenté [MB18]: Idem as previous comment

Incident: ~~A Network Incident is a~~An undesired Occurrence such as an unexpected interruption of a network service, degradation of the quality of a network service, or the below-target performance of a network service. An Incident results from one or more Problems, and a Problem may give rise to or contribute to one or more Incidents. Greater discussion of Network Incidents, including Incident management, can be found in [I-D.ietf-nmop-network-incident-yang].

Anomaly: ~~A (network) Anomaly is a~~An unusual or unexpected Event or pattern in network data in the forwarding plane, control plane, or management plane that deviates from the normal, expected behavior. See [I-D.ietf-nmop-network-anomaly-architecture] for more details.

Symptom: An observable Characteristic, ~~/~~State~~/~~, or Condition considered as an indication of a Problem or potential Problem.

Cause: The Events (Detected or otherwise) that gave rise to a Fault/ Problem.

Consolidation: The process of considering multiple Problems,

Commenté [MB19]: Can we cite Fault as well?

Symptoms, and their Causes to determine the underlying Causes.

Alert: ~~The~~ An indication of a Fault.

Alarm: Per [RFC8632], an Alarm signifies an undesirable State in a

Resource that requires corrective action(s). From a management point of view, an Alarm can be seen as a State in its own right and the transition to this State is a Fault and may result in an Alert being issued. The receipt of this Alert may give rise to a continuous indication (to a human operator) highlighting the potential or actual presence of a Problem.

3.3. Other Terms

Two other terms may be helpful:

Transient: A State, considered as a Problem, that persists for a limited amount of time before becoming resolved without direct action by an operator or by a system that controls or manages the network.

Intermittent: A State that is not continuous, but keeps occurring in some time frame.

4. Workflow Explanations

The relationship between System, Resource, and Characteristics is shown in Figure 1. A System is comprised of Resources, and Resources have Characteristics.

Commenté [MB20]: Any reason «s» is used here but not for «resourceS»?

A system may be composed of multiple resources as well.

```
Characteristics
       ^
       |
    Resource
       ^
       |
     System
```

Figure 1: Relationship Between Elements of a System

The Value of a Characteristic of a Resource ~~is expected to~~may change over time. Specific Changes in Value may be noticed at a specific time (as digital Changes), Detected, and treated as Events. This is shown on the left of Figure 2.

The center of Figure 2 shows how the Value of a Characteristic may change over time. The Value may be Detected at specific times or periodically and give rise to States (and consequently State Changes).

In practice, the Characteristic may vary in an analog manner over time as shown on the ~~right hand~~right-hand side of Figure 2. The Value can be read or reported (i.e., Detected) periodically leading to Analog Values that may be deemed Values with Relevance, or may be evaluated over time as shown in Figure 6.

Commenté [MB21]: I guess this is just an example. It does not need to be periodic.

```
          Event                State                 Value

            ^                    ^                     ^
     Detect :             Detect :              Detect :
            :                    :                     :

       ^        ^          ^     ^     ^                  /\
       :        :          :     :     :                 /  \
       :        :          :     :     :           /\   /    \
        __    __                _____             /  \/
       |        |              |     |          /\/
     __|        |__        ____|     |____     /

     Change at a time     Change over time     Change over time
```

Figure 2: Characteristics and Changes

Figure 3 shows the workflow progress for Events. As noted above, an Event is a Change in the Value of a Characteristic at a time. The Event may be evaluated (considering policy, relative to a specific perspective, with a view to intent, and in relation to other Events, States, and Values) to determine if it is an Occurrence and possibly to indicate a Change of State. An Occurrence may be undesirable (a Fault) and that can cause an Alert to be generated, may be evidence of a Problem and could directly indicate a Cause. In some cases, an Alert may give rise to an Alarm highlighting the potential or actual presence of a Problem.

Commenté [MB22]: FWIW, rfc8632 defines alarm as a state.

«An alarm signifies an undesirable state in a resource that requires corrective action »

Wonder if «give rise to» is consistent with that?

```
   Alert- - - - > Alarm
     ^
     |
     |     -----> Cause
     |     |
     |----------> Problem
     |
     |
   Fault
     ^
     |
     |
     |
 Occurrence
     ^
     |
     |----------> State
     |
     |
   Event
```

Figure 3: ~~Events~~Event and Dependent Terms

Parallel to the workflow for Event~~s~~, Figure 4 shows the workflow progress for State~~s~~. As shown in Figure 2, Change noted at a particular time gives rise to State. The State may be deemed to have Relevance considering policy, relative to a specific perspective, with a view to intent, and in relation to other Events, States, and Values. A State with Relevance may be deemed a Problem, or may indicate a potential Problem.

Commenté [MB23]: For consistency with a similar mention in the doc.

Problems may be considered as Symptoms and may map directly or indirectly to Causes. An Incident results from one or more Problems. An Alarm may be raised as the result of a Problem.

Commenté [MB24]: Check if this can be considered as a State

```
                     Alarm
                       ^
                       |     ------> Incident
                       |    |
                       |    |   ---> Cause
                       |    |   |
                   Problem---------> Symptom
                       ^
                       |
                       | Relevance
                       |
                       |
                     State
```

Figure 4: ~~States~~State and Dependent Terms

Figure 5 shows how Faults and Problems may be Consolidated to determine ~~the~~ (candidate) Causes. The arrows show how one item may give rise to another.

A Cause can be indicated by or determined from Faults, Problems, ~~and~~ and Symptoms. It may be that one Cause points to another, and can also be considered as a Symptom. The determination of Causes can consider multiple inputs. An Incident results from one or more Problems.

```
                               ---------
                 ------------- |       |
                |  ----------> | Symptom |
                | |            |       |
                | |             ---------
                v |                 ^
             ---------              |
    ------->|  Cause  |<---------   |
   |         ---------          |   |
   |            ^    |          |   |
   |            |    |          |   |
   |             ---            |   |
```

```
                |                             |  |
            ---------                      ---------          ----------
           |  Fault  |------------------->| Problem |------->| Incident |
            ---------                      ---------          ----------
```

                  Figure 5: Consolidation of Symptoms and Causes

~~The final figure in this section (~~Figure 6~~)~~ shows how thresholds are important in the consideration of Analog Values and Events. The arrows in the figure show how one item may give rise to or utilize another. The use of threshold-driven Events and States (and the Alerts that they might give rise to) must be treated with caution to dampen any "flapping" (so that consistent States may be observed) and to avoid overwhelming management processes or systems. Analog Values may be read or notified from the Resource and could transition a threshold, be deemed Values with Relevance, or evaluated over time. Events may be counted, and the Count may cross a threshold or reach a Value of Relevance.

The Threshold Process may be implementation-specific and subject to policies. When a threshold is crossed and any other conditions are matched, an Event may be determined, and treated like any other Event.

```
       Occurrence
            ^
            |
            |---------------------> State
            |
            |        -------                 Relevance
            |------>| Count |-----------------------------> Value
            |        -------          |                       ^
            |           |             |                       |
            |           |             |                       | Relevance
            |           |             v                       |
            |           |        -----------           ----------------
          Event         |       | Evaluated |         |                |
            ^           |       | over time |<--------|  Analog Value  |
            |           v        -----------          |                |
            |      -----------        |               |                |
            |     | Threshold |       |               |                |
            |<----|  Process  |<------                |                |
            |     |           |<----------------------|                |
            |      -----------                         ----------------
            |                                                 ^
            |                                                 |
            | Detect                                   Detect |
            |                                                 |
       Change at a Time                                Change over Time
```

                     Figure 6: Counts, Thresholds, and Values

5. Security Considerations

This document specifies terminology and has no direct effect on the security of implementations or deployments. However, protocol solutions and management models need to be aware of several aspects:

* The exposure of information pertaining to Faults may make available knowledge of the internal workings of a network (in particular its vulnerabilities) that may be of use to an attacker.

* Systems that generate management information (messages, notifications, etc.) when Faults occur, may be attacked by causing them to generate so much information that the system that manages the network is swamped and unable to properly manage the network.

* Reporting false information about Faults (or masking reports of Faults) may cause the system that manages the network to function incorrectly.

Examples of security considerations relevant to specific network management protocols can be found in Section 5 of [RFC6632].

6. Privacy Considerations

In general, Fault Management should not expose information about end-user activities or user data. The main privacy concern is for a network operator to keep control of all information about Faults to protect their privacy and the details of how the network operators operate their network.

7. IANA Considerations

This document makes no requests for IANA action.

Acknowledgments

The authors would like to thank Med Boucadair, Wanting Du, Joe Clarke, Javier Antich, Benoit Claise, Christopher Janz, Sherif Mostafa, Kristian Larsson, Dirk Hugo, Carsten Bormann, Hilarie Orman, Stewart Bryant, and Paul Kyzivat for their helpful comments.

Special thanks to the team that met at a side meeting at IETF-120 to discuss some of the thorny issues:

* Benoit Claise

* Watson Ladd

* Brad Peters

* Bo Wu

* Georgios Karagiannis

* Olga Havel

* Vincenzo Riccobene

* Yi Lin

* Jie Dong

* Aihua Guo

* Thomas Graf

* Qin Wu

* Chaode Yu

* Adrian Farrel

Informative References

[DimensionalModeling]
Wikipedia, "Dimensional Modeling", 18 November 2024, <https://en.wikipedia.org/w/index.php?title=Dimensional_modeling>.

[I-D.ietf-nmop-network-anomaly-architecture]
Graf, T., Du, W., and P. Francois, "An Architecture for a Network Anomaly Detection Framework", Work in Progress, Internet-Draft, draft-ietf-nmop-network-anomaly-architecture-01, 20 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-nmop-network-anomaly-architecture-01>.

[I-D.ietf-nmop-network-incident-yang]
Hu, T., Contreras, L. M., Wu, Q., Davis, N., and C. Feng, "A YANG Data Model for Network Incident Management", Work in Progress, Internet-Draft, draft-ietf-nmop-network-incident-yang-02, 10 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-nmop-network-incident-yang-02>.

[RFC3877] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, DOI 10.17487/RFC3877, September 2004, <https://www.rfc-editor.org/info/rfc3877>.

[RFC8632] Vallin, S. and M. Bjorklund, "A YANG Data Model for Alarm Management", RFC 8632, DOI 10.17487/RFC8632, September 2019, <https://www.rfc-editor.org/info/rfc8632>.

[RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <https://www.rfc-editor.org/info/rfc9232>.

[RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, October 2022, <https://www.rfc-editor.org/info/rfc9315>.

Authors' Addresses

Nigel Davis (editor)

Ciena
United Kingdom
Email: ndavis@ciena.com

Adrian Farrel (editor)
Old Dog Consulting
United Kingdom
Email: adrian@olddog.co.uk

Thomas Graf
Swisscom
Binzring 17
CH-8045 Zurich
Switzerland
Email: thomas.graf@swisscom.com

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Chaode Yu
Huawei Technologies
Email: yuchaode@huawei.com