International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.475

(01/2020)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

Network management – Checking the quality of the international telephone service

Guidelines for intelligent network analytics and diagnostics

Recommendation ITU-T E.475

International Telecommunication Union

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

INTERNATIONAL OPERATION	
Definitions	E.100–E.103
General provisions concerning Administrations	E.104–E.119
General provisions concerning users	E.120–E.139
Operation of international telephone services	E.140–E.159
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.189
Numbering plan of the international telephone service	E.190–E.199
Maritime mobile service and public land mobile service	E.200–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	
Charging in the international telephone service	E.230–E.249
Measuring and recording call durations for accounting purposes	E.260–E.269
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	
General	E.300–E.319
Phototelegraphy	E.320–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.349
INTERNATIONAL ROUTING PLAN	E.350–E.399
NETWORK MANAGEMENT	
International service statistics	E.400–E.404
International network management	E.405–E.419
Checking the quality of the international telephone service	**E.420–E.489**
TRAFFIC ENGINEERING	
Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.649
Traffic engineering for IP-networks	E.650–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	
Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899
OTHER	E.900–E.999
INTERNATIONAL OPERATION	
Numbering plan of the international telephone service	E.1100–E.1199
NETWORK MANAGEMENT	
International network management	E.4100–E.4199

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T E.475

Guidelines for intelligent network analytics and diagnostics

Summary

With the increased number of connected devices and the proliferation of web and multimedia services, cloud services and Internet of things (IoT) applications, networks are subject to various network incidents and unregulated network changes which may be measured by network alerts and logs received from the underlying networks. Therefore, it is important for the networks to be aware of the services and applications they transport to optimize the operation and ensure that service quality meets user expectations. The absence of network alerts or network logs is generally interpreted as an indication of good network health. However, this is not necessarily the case. Service quality problems may not be the result of network device failures, but instead due to issues that are not detected by traditional network monitoring tools such as configuration errors, insufficient network capacity, wireless access point issues (e.g., insufficient coverage, interference or overlapping channel), or third party network issues.

Typically, the manual network reconfiguration is time consuming and often error prone. In addition, service quality assessment methodologies need to further distinguish between network impairments and other causes of the performance degradation by considering application-specific factors (e.g., encoding/decoding, interaction between an application and a network) as the traditional assessment tools cannot provide accurate fault diagnosis, fault prediction, and root cause analysis. Furthermore, the reaction time of traditional assessment tools tends to be slow, responding after the service disruption occurs. In addition, the network performance metrics may contribute to quality of service/quality of experience (QoS/QoE) assessment, but many of the existing network performance metrics may reflect only limited aspects of the network quality.

When the objectively-measured results indicate an unsatisfactory level of network performance or anomaly degree, it is desirable that the system performs the necessary corrective actions automatically to resolve the identified quality problems.

Recommendation ITU-T E.475 specifies guidelines for intelligent network analytics and diagnostics for managing and troubleshooting networks. The intelligent network analytics and diagnostics (INAD) function is responsible for aggregating network data and setting up automatic tasks for network maintenance, providing the assurance of appropriate network performance, locating the service degradation area and service channels with poor performance, finding root causes of the detected network faults, probing network status, and predicting the possible network performance degradation at an early stage.

Specifically, this Recommendation describes the design considerations, functional architecture, network anomaly analysis models for network analytics and diagnostics. The network anomaly analysis model can be used to assess network anomaly degree, network performance, risk degree, to analyse the location and time of the network impairment and further to determine the root causes of the network impairments and to allow increased network visibility and network fault management automation.

This Recommendation also presents the concept of network health indicator (NHI) which provides a numerical indication of the network anomaly degree based on dig data analytics. The NHI is not focused on a specific multimedia application rating (e.g., rating of specific audio application, video conferencing application) and application layer monitoring. Instead, it aims at network monitoring and evaluation of specific networks (e.g., LAN, WAN, storage network, data centre network) and further triggers network diagnosis using big data based fault diagnosis algorithms and determine the root causes of the network anomaly events.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T E.475	2020-01-13	12	11.1002/1000/14148

Keywords

Diagnostics, IP network services, network analytics, QoE, QoS.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T E.475

Guidelines for intelligent network analytics and diagnostics

1 Scope

With the increased number of connected devices and the proliferation of web and multimedia services, cloud services and IoT applications, the network are subject to various network incidents and unregulated network changes which are measured by network alerts and logs received from the underlying networks. Therefore, it is important for the network to be aware of the services and applications it facilitates when users are experiencing audio/video quality related problems and to operate the network to ensure that the offered services meet user expectations on service quality. The absence of network alerts or network logs is generally interpreted as an indication of good network health. However, service quality problems may not be the result of network device failures but the result of configuration errors, insufficient network capacity, wireless access point issues (e.g., insufficient coverage, interference or overlapping channel), or third party network issues, and these issues may not be detected by traditional network monitoring tools. Typically, the manual reconfiguration is time consuming and often error prone. In addition, service quality assessment methodologies need to further distinguish between network impairments and other causes of performance degradation by considering application-specific factors (e.g., encoding/decoding, interaction between an application and a network) because the traditional assessment tools cannot provide accurate fault diagnosis, fault prediction, and root cause analysis. Moreover, they usually respond to the network event slowly after the service disruption. In addition, the network performance metrics may contribute to QoS/QoE assessment, but many of the existing network performance metrics may reflect only limited aspects of the network quality.

The objective of this Recommendation is to describe the guidelines for intelligent network analytics and diagnostics for managing and troubleshooting networks. The guidelines derive its assessment from the analysis of data collected from networks and address the quality assessment of network anomalies based on data collected from the network. The network data can be in the form of network logs, network configuration data, service platform data, call details record (CDR), traffic statistics, alerts or performance data.

This Recommendation covers the following:

- Design consideration,
- Functional architecture overview,
- Network analytics and diagnostics methodology,
- Network analytics and diagnostics models,
- Network risk analysis by leveraging the key performance indicators (KPIs') correlation and the association between user experience and network performance,
- Network analytics and diagnostics applications.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [b-ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.3 big data [b-ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

3.1.4 big data as a service (BDaaS) [b-ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are ability to collect, store, analyse, visualize and manage data using big data.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 log event: A log event refers to a message in a log file, which can be considered as an occurrence of an atomic network event.

3.2.2 log template: A log template refers to a pattern or a collection of core keywords that describes the setting of a specific device and the conditions of its processes.

3.2.3 clustering: The process of partitioning a set of patterns into disjoint and homogeneous meaningful groups.

NOTE – Definition based on [b-Mining-Clustering].

3.2.4 natural language processing: The process of converting a piece of English text into a programmer-friendly data structure that describes the meaning of the natural language text.

The natural language processing tasks include part-of-speech tagging, chunking, named entity recognition, and semantic role labelling.

NOTE – Definition based on [b-NLP].

3.2.5 keyword extraction: Automatic identification of terms that best describe the subject of a document.

NOTE – Definition based on [b-keyword-Extraction].

3.2.6 telemetry: A mechanism that provides a continuous stream of data from the devices within a network to a set of receiving equipment for analysis task.

3.2.7 pattern: The aspects of data commonly described in terms of centre, spread, shape, and unusual features. Two of the most common unusual features are gaps and outliners.

3.2.8 gaps: Areas of a distribution where there are no observations.

3.2.9 outliers: Values that are sometimes present in distributions that are characterized by extreme values that differ greatly from the other observations.

3.2.10 centre: The centre is located at the median of the distribution.

3.2.11 spread: The propagation of a distribution that refers to the variability of the data.

NOTE – If the observations cover a wide range, the spread is larger. If the observations are clustered around a single value, the spread is smaller.

3.2.12 shape: The symmetry, number of peaks, skewness and uniformity of a distribution.

3.2.13 symmetry: An even distribution that can be divided at the centre so that each half is a mirror image of the other.

3.2.14 peaks: The point of a normal distribution curve with the maximum value.

NOTE – Distributions with one clear peak are called unimodal, and distributions with two clear peaks are called bimodal.

3.2.15 skewness: A measure of the asymmetry of the density of observations done on two different sides of a graph resulting in the distribution of more observations on one side of the graph than the other.

3.2.16 uniform: Characteristics of a distribution where the observations in a data set are equally spread across the range of the distribution.

NOTE – A uniform distribution has no clear peaks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APN Access Point Name

BDaaS Big Data as a Service

BGP Border Gateway Protocol

CDR Call Details Record

CPU Central Processing Unit

DSCP Differentiated Services Code Point

DSLAM Digital Subscriber Line Access Multiplexer

EWMA Exponentially Weighted Moving Average

FTTx Fiber To The x

Gi Guard interval

GPON Gigabit-capable Passive Optical Networks

HDFS Hadoop Distributed File System

INAD Intelligent Network Analytics and Diagnostics

IoT Internet of Things

IOAM In-situ Operations, Administration, and Maintenance

IPTV Internet Protocol Television

KPI Key Performance Indicator

KQI Key Quality Indicator

MOS Mean Opinion Scores

NHI Network Health Indicator

NTP Network Time Protocol

OLT Optical Line Terminal

ONT Optical Network Terminal

OSPF Open Shortest Path First

OSS Operations Support System

OTT Over The Top

PCA Principal Component Analysis

PDN Packet Data Network

QoE Quality of Experience

QoS Quality of Service

RAN Radio Access Network

SGi Short Guard interval

TCP Transmission Control Protocol

TF-IDF Term Frequency – Inverse Document Frequency

UDP User Datagram Protocol

VAP Very Annoyed Person

VLAN Virtual Local Area Network

VoLTE Voice over Long-Term Evolution

WDM Wavelength Division Multiplexing

xDSL x Digital Subscriber Line

5 Conventions

In this Recommendation, the keyword "**must**" is a mandatory term indicating a condition or behaviour that is an absolute requirement of this Recommendation. The keyword "**should**" is a normative term indicating that there may exist valid reasons in particular environment to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different condition or behaviour.

The keyword "**may**" is a normative term indicating an optional condition or behaviour.

The keyword, "**can**" is an informative term indicating a condition or behaviour that will potentially be encountered within the environment to which this Recommendation applies.

6 Design considerations

The objective of this Recommendation is to look beyond existing off-the-shelf data processing techniques, and build real-time automatic analytics and visualization tools which can:

1) Provide the ability to gain insights from the vast amount of network data,
2) Transform these insights into values that can be beneficial to network maintenance and operations in practice.

6.1 Consideration for data collection

The increased number of connected devices and the proliferation of web and multimedia services imposes a great impact on the network. Therefore, the network may be subject to increased network incidents and unregulated network changes without network visibility or a clear view of the available network resources and network topology. Thus, to provide rapid network diagnosis, the vast amount of data should be gathered from the network in a speedy manner.

Data collection implies information collection from various data sources (e.g., event, metric, in-situ, etc.) using a set of automated communication processes, and the collected data is transmitted to one

or more receiving systems for analysis. Data collection is a systematic approach to gathering and measuring information from a variety of sources to get a complete and accurate picture of the network. Network devices are required to collect network event data, metric data, in-situ data and report the data.

6.2 Data processing techniques

The data processing techniques in these guidelines focus on four aspects, as illustrated in Figure 6-1:

1) Make information available for real-time monitoring and play out check,
2) The ability to link data and to correlate various data sources to gain a more comprehensive view of the network system,
3) Filter data according to the needs while retaining the ability to find a needle in the haystack during trouble shooting,
4) Transform data into models and benchmarks, which in turn provides improved understandings of the network system status and recommendations for future actions and practices.

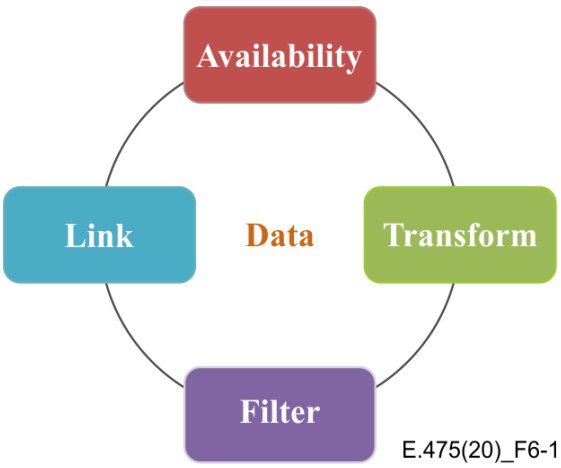


Figure 6-1 – Data processing techniques

6.3 Data analytics and diagnostics

To fully exploit the insights gleaned from the network data and to create values to support network maintenance and operation, this clause lists the key areas where these guidelines can transform insights into values, as illustrated in Figure 6-2:

6.3.1 Network maintenance

The following are key areas for network maintenance that can be used to transform insights into values:

1) Automated: provide tools for automatically aggregating the network data and setting up automatic tasks for network maintenance.
2) Reactive: dimension issues and find root causes when network faults are detected.
3) Proactive: actively probe the network status and predict possible network performance degradation at an early stage.

6.3.2 Network operation

The following are key areas of a network operation that can be used to transform insights into values:

1) Ensure: real-time monitoring that provides assurance of appropriate network performance.

2) Optimize: locate service degradation area and service channels with poor performance which need optimization.

3) Enrich: observe and predict traffic patterns in order to provide better service experiences.

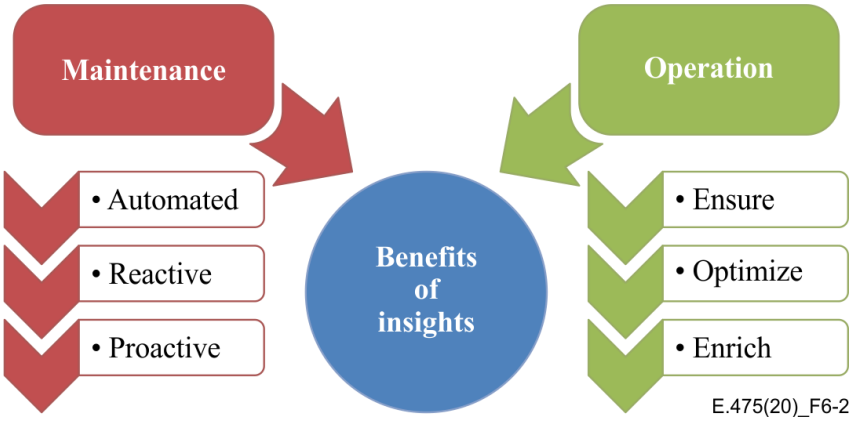


Figure 6-2 – Data analytics and diagnostics

7 Functional reference architecture for intelligent network analytics and diagnostics

Figure 7-1 shows the incremental high-level functional architecture required for intelligent network analytics and diagnostics (INAD) abilities in the data analytics level and data diagnostics engine level.

The network analytics and diagnostics abilities shown in Figure 7-1 can be in the form of two major functions, which are the network analytics function and network diagnostics function. The network analytics function is used to aggregate the network data, set up automatic tasks for network maintenance, provide assurance of appropriate network performance, anticipant network event, and perform trend analysis. The network diagnostics function is used to forecast short term changes and risks in the network, locate service degradation areas and service channels with poor performance that needs optimization, and find root causes when network faults are detected. In addition, this functional reference architecture also includes a data collection function at the data sources level. Through interaction with these functional components, it is possible to coordinate monitoring tasks, detect degraded network performance, conduct proactive risk assessments of network quality, which can form closed loop control, make decision, operate and optimize the network to meet on-demand service requirements.

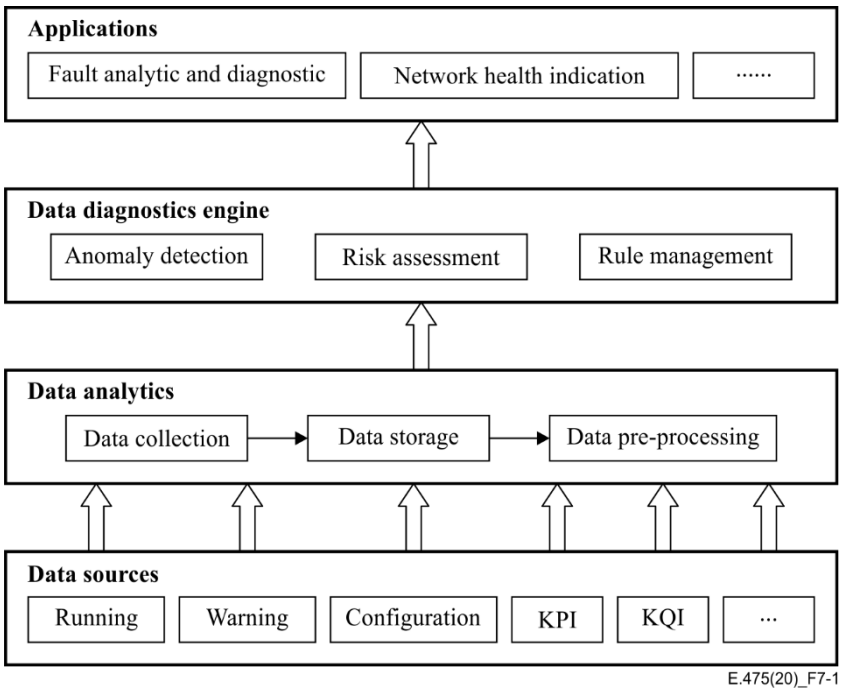


Figure 7-1 – INAD functional reference architecture

7.1 Data sources

The data exchanged between users of communication services on the user plan (voice, text) is considered as private content and is generally not captured by operators. However, the data can be collected if necessary (e.g., for legal interception) from the following sources:

1) Fixed access network

   Fixed access can be fibre based (FTTx) or copper based (xDSL). In both cases, some connection and traffic logs are available on the anchor point (DSLAM, GPON OLT).

   If the services are differentiated on the network (different VLAN or differentiated services codepoint (DSCP)), some KPIs per service are available, mainly focused on the network QoS.

2) Fixed core network

   Probes are often present inside the fixed core network, and they collect some KPIs per service, available in central collection databases.

3) Mobile access network

   i) RAN counters

      Counters extracted from eNodeB (4G), RNC (3G) and BTS/BSC (2G) are available a posteriori. This is not available in real time. It is generally averaged over a 15 min timeframe.

      Operations support system (OSS) gathers all counters extraction on data volume, the number of voice calls, call drop ratio, call success ratio, etc.

      Please note that these KPIs are not provided per user but aggregated per cell instead. It can also be per service if the service is differentiated at the RAN level (e.g., VoLTE is using a specific bearer).

      A possible improvement could be to calculate voice mean opinion score (MOS) at RAN level and to gather them per user and per location at the OSS.

   ii) Probe on transport interface

Some probes can be placed on the interface between the RAN and core network in order to log all media and signalling. This is intended first for troubleshooting: the volume of traces is large and traces cannot be logged permanently. In the future, it may be possible to log more information than only aggregated data, such as user location, type of service, user experience (e.g., web page download time), etc.

4) Mobile packet core network

   i) Counter/logs on the packet data network (PDN) gateway

      Some logs are available on PDN gateways, and they contain some particular information on the access point name (APN). Most of these statistics can be seen also with probes on dedicated interfaces (e.g., Gi/SGi).

   ii) Probe on Gi/SGi interface

      Raw data collected by probes are generally stored and available for a few days only. It is also processed in order to store aggregated information for a longer period of time, in the form of usage statistics on 6-month time windows, for example.

5) Use of user location information

   User location can be determined by GPS, cell tower information, access point, etc.

In the network context, a data source is any of the following types of sources for, mostly, digitized data. Logging allows the monitoring of the state of network devices, services, ports or protocols.

The corresponding log data can be classified into three categories:

1) Event type, such as 'Running', 'Warning', 'Configuration', etc.
2) Metric type, such as 'KPI', 'KQI', etc.
3) In-situ type, such as 'IOAM', etc.

The following clauses describe the characteristics of these data types.

7.1.1 Event type

Logging event types provide critical information on network device failures and troubles and may also provide descriptions of routine network activities such as interface flapping, border gateway protocol (BGP) statistics data, and open shortest path first (OSPF) statistics data.

The logs can also carry metrics information besides events. However, this clause only discusses events description. Metrics description is discussed in clause 7.1.2.

Log events data has the following characteristics:

- Timestamp characteristics: in addition to recording event timestamps, i.e., the time at which network events occurred, a detection of network anomaly can be performed by monitoring the timestamp pattern, i.e., how timestamps vary over time. Timestamp pattern monitoring can be done in several ways:
  - The time interval between two consecutive network events can be tracked and monitored for consistency.
  - The order in which network event occurs can be tracked and monitored for consistency.

  Consistency would indicate normal conditions, and deviations would usually indicate network anomaly happening on specific network devices.
- Density characteristics: in normal conditions, very few logs are generated but in an abnormal condition, the network devices may generate a greater amount of network logs.
- Severity rank characteristics: each record event data is labelled with a severity rank. In Syslog, PRI field could be used to describe the severity rank of the event data, which can be obtained from standard protocols or mechanisms.

- Log type characteristics: if a network device is malfunctioning, it is likely that its hardware or software would be in an abnormal condition and would generate new types of network or log events.
- Pattern characteristics: log pattern characteristics refers to the correlation between network events. Suppose a network protocol running on the network device has three log events, i.e., log event A, log event B, log event C corresponding to three states in the state machine of the network protocol. In the normal condition, the log event mode will follow the order A->B->C. When the log event mode changes the order such as B->A->C, it is more likely that the network device is malfunctioning. This technique is similar to the timestamp pattern monitoring presented above.
- Key log event: a blacklist of some key log events can be defined for network devices. When a key event log occurs on a specific network device, it is likely that the network device is broken or malfunctioning.
- Similarity characteristics: similarity characteristics can be extracted by comparing logs from two adjacent network devices, or two series of log events from the same network device on different time periods. Differences in similarity may indicate network anomaly. Temporal and spatial characteristics should be taken into account while performing similarity characteristics analysis.

7.1.2 Metrics type

Network metrics data represents the operational state of a network device, link or network protocol in the network. Metric data is usually represented to users as a set of time series (e.g., $Metric = x_i$, $i = 1,2, \dots, t$), where each time series corresponds to one network metric value at different time point during a specific time period. The analysis of the statistical characteristics can be used to identify the time point at which the data is abnormal or risky. The statistical characteristics include but is not limited to:

- Mean: the average of the time series data.
- Variance: the degree of dispersion of the time series data.
- Component sequences: the time series of network metric that can be decomposed into the additive combination of different component sequences by some mathematical processing methods.
- Data similarity: the similarity between two time series. An example of commonly used similarity measure is the cosine similarity.
- Statistic value: the value obtained by some functional operation (e.g., statistical algorithm) on the data.

The following characteristics could be derived from the metrics data:

- Fluctuation characteristic: fluctuation is an important indicator to measure the accuracy of the health status of the network element. It shows the statistical index which rises and falls sharply over a period of time and indicates whether the state of the network element is stable.
- Trend characteristic: trend is an important indicator for measuring the accuracy of the health status of the network element. Theoretically, metric data is collected based on the acquisition time and acquisition frequency, and the trend component can be obtained by decomposing the data that has been timestamp ordered. When the state of a network element is in the process of deterioration, rising or falling trend would be observed.
- Threshold characteristics: thresholds are also important indicators to measure the health status of the network element. Thresholds can be derived from the range of metric values collected on a specific network element.

7.1.3 In-situ type

IOAM (in-situ OAM) is a measurement mechanism to record operational information in the packet while the packet travels from one node (host or router) to the subsequent node (host or router) along a path. It defines a mechanism for adding telemetry data to the data plane packets.

The term "in-situ" refers to the fact that the OAM and telemetry data is carried within data packets rather than being sent within packets specifically dedicated to OAM. IOAM data includes the telemetry data and OAM information along the path within the data packet. In-situ OAM is capable of embedding metadata, such as node identifiers, identifiers which the packet was received and sent-out on, ingress and egress timestamps in the forwarding plane packets.

7.1.3.1 IOAM data types

The different uses of IOAM require the definition of different types of data. The information gathered for IOAM can be categorized into three main categories, i.e., edge-to-edge, per node, and selected nodes.

- "edge to edge": This category includes the information that needs to be shared between network edges (the "edge" of a network could either be a host or a domain edge device). Edge-to-edge data, e.g., packet and octet count of data entering a well-defined domain, the sequence number (also called "path packet counters") is useful for the flow to detect packet loss.
- "selected nodes": This category includes the information that applies to a specific set of nodes only. In case of path verification, only the nodes which are "check points" are required to interpret and update the information in the packet.
- "per node": This category includes the information that is gathered at every hop along the path that a packet traverses within an administrative domain. This includes two kinds of information, hop-by-hop information and inherent information. Hop-by-hop information is the information that nodes used for path tracing, e.g., timestamps at each hop to find delays along the path. Inherent information is the statistic collection at each hop to optimize communications in resource constrained networks, e.g., battery, central processing unit (CPU), memory status of each node.

7.1.3.2 IOAM data attribute

In this clause, a set of IOAM data fields and their associated attributes are described.

- Hop_Lim: It is set to the hop limit value in the packet at the node that records this data (applicable for protocols like IPv6 which include a hop limit field in their header). Hop limit information is used to identify the location of the node in the communication path.
- node_id: 3-octet unsigned integer. Node identifier field to uniquely identify a node within an IOAM domain.
- ingress_if_id: 2-octet unsigned integer. Interface identifier describing the ingress interface where the packet was received.
- egress_if_id: 2-octet unsigned integer. Interface identifier describing the egress interface from which the packet is forwarded.
- timestamp seconds: 4-octet unsigned integer. Absolute timestamp in seconds that specifies the time at which the packet was received by the node.
- timestamp nanoseconds: 4-octet unsigned integer in the range 0 to 10^9-1. This timestamp specifies the fractional part of the wall clock time at which the packet was received by the node in units of nanoseconds.
- transit delay: 4-octet unsigned integer in the range 0 to 2^31-1. It is the time in nanoseconds that the packet spent in the transit node.

- app_data: 4-octet data field which can be used to add application specific data.
- queue depth: 4-octet unsigned integer field. It indicates the current length of the egress interface queue of the interface from which the packet is forwarded.

7.2 Data analytics

Data analytics refers to the processes of collecting and manipulating raw data to yield useful information. Data analytics is also the conversion of raw data into machine-readable form and its subsequent processing by a computer. It involves data collection, storage and presentation of the desired information.

However, the ability to extract and load high-volume data does not directly lead to high-quality data. The data analytics functions also play a vital role to purge the raw network data (e.g., removing invalid data and handling missing data), correlate data across heterogeneous entities, and filter data according to specific applications and time range under consideration. Clauses 7.2.1 to 7.3 describes these stages.

7.2.1 Data collection

In the phase of data collection, an INAD management system needs to both pull data that has already been generated from data source on network devices (offline data collection) and collect a continuous stream of data from the devices within a network (online data collection). For online data collection, automated proactive probe tasks or measurement tasks may need to be set up to collect telemetry data, and an INAD management system may allow a subscriber to select portions of the data, push of data synchronously or asynchronously via registered subscriptions.

An INAD management system needs to retrieve data from various data sources: logs, trouble tickets, device configuration files, metrics, and network telemetry data source. Such data collection sub-system should be highly-scalable but light-weighted, which in turn can support high throughput data collection task without incurring too much overhead for the network operation.

Syslog is a message logging standard. Since most network devices support Syslog protocols to send log information, Syslog is also a commonly used mechanism to retrieve logs from network devices by network administrators.

An INAD management system could use a syslog server to collect logs and feed data to data analytics and diagnostics components via database queries. A syslog server is a server that supports using syslog protocol to retrieve and aggregate logs from multiple sources, which consists of two core components as shown in Figure 7-2:

- A Syslog listener: A syslog server needs to receive messages sent over the network. A listener process gathers syslog data sent over UDP port 514 or TCP port 1468.
- A database: Large networks can generate a huge amount of syslog data. A syslog server uses a database to store syslog data for storing and quick retrieval. The syslog data comprise various types of data, such as, event data, configuration data, metric data, and alarm data.

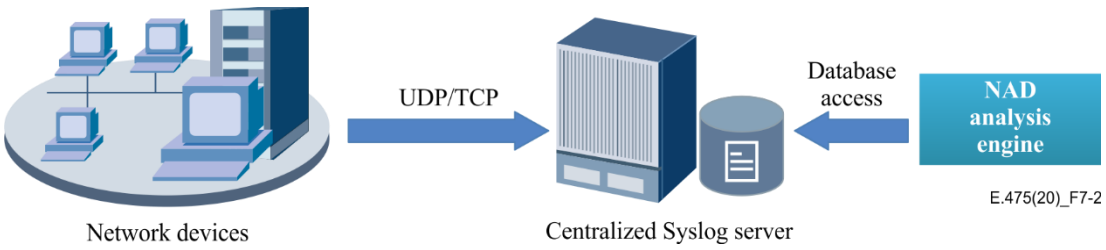


Figure 7-2 – Log data collection

7.2.2 Data storage

As different types of data are collected, they can either be written directly (in real time) into memory processes or can be written to disk as messages, files, or database transactions. Once received, there are multiple options on where to put the data. It can be written to the file system, traditional relational database management system (RDBMS), or distributed clustered systems such as NoSQL and Hadoop distributed file system (HDFS). The primary techniques for rapid evaluation of unstructured data is by running batch or stream processing, agnostic of map-reduce.

7.2.3 Data pre-processing

Currently, data-gathering methods are often loosely controlled, resulting in out-of-range values, missing values, impossible data combinations (e.g., Sex: Male, Pregnant: Yes), etc. Network data are highly susceptible to noisy, missing, and inconsistent data due to big volume, multiple, and heterogeneous sources.

Mining of high value information from poor quality data is difficult. Data pre-processing is an important step in the data mining process. However, how can the data be pre-processed in order to help improve the quality of the data and, consequently, of the mining results? How can the data be pre-processed to improve the efficiency and ease of the mining process?

There are several kinds of data pre-processing techniques:

- Data cleaning: It can be applied to remove noise and correct inconsistencies in data.
- Data integration: It merges data from multiple sources into a coherent data store such as a data warehouse.
- Data reduction: It can reduce data size by, for instance, aggregating, eliminating redundant features, or clustering.
- Data transformations: It (e.g., normalization) may be applied, where data are scaled to fall within a smaller range like 0.0 to 1.0. This can improve the accuracy and efficiency of mining algorithms involving distance measurements.

These techniques are not mutually exclusive as they may work together. For example, data cleaning can involve transformations to correct incorrect data by transforming all entries for a date field to a common format.

To convert a large volume of data to high-value information for network management, it is necessary to integrate network-specific rules and knowledge into data pre-processing components and to introduce domain expertise into the network analytics and diagnostics system. The analytics and diagnostics system will then be able to provide insights for network maintenance and potential network problems.

7.3 Data diagnostics engine

The data diagnostics engine uses network data analysis to improve the ability of fault localization and diagnosis. It consists of three major components, i.e., anomaly detection, risk assessment, and rule management.

7.3.1 Anomaly detection

In the data diagnostics engine, anomaly detection is the identification of items, events, metric, flows or state anomalies which do not conform to an expected pattern or other items in a network dataset. Typically, the anomalous items is likely to trigger events in logs, configurations, metrics or alarms.

Anomaly detection module is responsible for handling network faults by various different means, e.g., analysing trouble tickets, logs and associated telemetry of failure network devices, etc. The goal of anomaly detection is to apply telecom-specific logic (data models, rules sets, etc.) to automatically dimensioning issues and find the root causes of the network problems timely.

7.3.2 Risk assessment

In the data diagnostics engine, risk assessment is a component aiming at providing an estimation of the overall network risk condition. Unlike the anomaly detection component that deals with network faults and failure that already happened, the goal of risk assessment is to predict network events, forecast short term changes and risks in the network based on the trends of network data (e.g., fast growing, fast dropping, slowly increasing, or slowly decreasing of metric data). This opens up a channel to reveal potential network problems or locate the need for optimization and upgrade.

7.3.3 Rule management

In the data analytics engine, expertise rules database is an evolving set of rules that keeps updating the network-specific domain knowledge and provides suggestions or recommendations on action to take to recover from network failures or past issues.

7.4 Applications

After the data goes through the generic processing stage, it is ready for domain-specific analytics to support various applications. An INAD architecture should support various applications such as network diagnostics application that uses the anomaly detection module of data analytics engine to find the root causes of the network problems timely, and the network health indication that uses the risk assessment module of the data diagnostics engine to provide a real-time indication of network health information.

8 Network diagnostics methodology

In INAD system analysis, there are usually two dimensions along which a system can be considered. These are time and spatial dimensions. It is within these two dimensions that the level of accuracy and the scales in which the system is analysed are chosen.

8.1 Spatial dimension anomaly analysis

The spatial dimension represents how the anomaly is analysed within the network topology, what spatial components are identified, what are the spatial borders of the data and what are the links to other data across the borders.

8.2 Temporal dimension anomaly analysis

The temporal dimension describes the level of resolution for data dynamics in time, the time step of analysis, and the temporal events that should be either singled out or grouped together.

The temporal scale for evaluating the abnormality of the network also gives additional insight. The temporal dimension shows the dynamics of network data, how and why they change in time. It may be interesting to compare the sustainability notion with that of stability.

9 Network analytics and diagnostics models

9.1 Network anomaly assessment models

Anomaly detection models are used to identify outliers, or unusual cases, in the data.

9.1.1 Network log-based anomaly detection model

Logging allows monitoring the states of network devices, services, ports or protocols. More importantly by analysing the logs of various devices in a network, the network can troubleshoot and optimize, and a comprehensive understanding of the global state of the network can be gained.

9.1.1.1 Network log-based analytics

Network logs analytics procedure includes data collection, data storage and data manipulation. Syslog is a valuable tool to retrieve logs and transport them to the analysis engine. However, in practice, it does not guarantee the fulfilment of the retrieval of all device logs. Devices that use UDP may sometimes fail to send syslog messages to a syslog server due to network congestion. The syslog server itself is susceptible to network attacks. Therefore, there is no guarantee that all messages are collected via this method since logs are generated from various devices, and each log format is defined by each device vendor. This is not a consistent structure of a specific type of devices' log files. Moreover, since a network is a distributed system, the time clocks on devices might not be synchronized, this may cause the timestamps in syslog files to be inconsistent as well. All these issues pose hurdles to analyse log files. The following text describes data filtering and correlating techniques for addressing these problems.

- Data filtering:

Log message are intertwined with both unstructured human-readable texts and structured machine-readable fields. Human-readable texts in log files describe the conditions of network processes, including alerts and notifications, while the machine-readable fields are often numeric fields that use standard convention to indicate basic information of a log. For example, syslog uses facility to refer to the type of the network device which the log sender belongs to. A facility of "0" would be a Kernel message, and a facility of "11" would be an FTP message. Syslog also has a field to denote the severity level of a log event. The severity level indicates how important the message is deemed to be. A severity of "0" is an emergency, "1" is an alert that needs an immediate action, and the scale continues right down to "6" and "7" – informational and debugs messages.

To support the analysis of log messages or log files saved on different type of devices, it is important to extract the critical information from logs and filter out noisy trivial information since these log files or the log message does not provide consistent storage format (e.g., CSV format, txt format, log format) for data elements defined in syslog message [b-RFC5424]. To do so, it is necessary to construct a unified log template to provide consistent data representation for data element collected from each type of devices. The construction of such log templates is not trivial, it should be automatic as well as support various log formats defined by different vendors. Natural language processing techniques can be leveraged and keyword extraction techniques such as TF-IDF to extract the core terms appearing in log files stored in various devices.

- Data correlating:

To gain the full picture of the network state, it is critical to understand causal relationships between log events and in turn help figure out the root causes for network problems. Capturing the relationships between log events that occurred before is not trivial. Sometimes, systems in the network are distributed without the NTP time server and hence the clocks on each device are not synchronized. To ensure the alignment of timeline in network logs, they could be associated across devices by the following procedure:

1) Logs from multiple network devices are collected for analysis.
2) Process each log file captured from each type of device to extract the discriminative features in the log files, e.g., time point of network anomaly, concurrent log events (i.e., the same type of log event that occurred at different devices simultaneously), the log event in proper order. There are many features in each network device.
3) Find the most relevant correlated feature across devices with the discriminative features extracted from individual logs, e.g., time point of network anomaly. The most relevant correlated feature refers to the correlated feature of many network devices.
4) Align all logs with the unified timeline according to the correlated features, e.g., time point of network anomaly. Firstly, record the reference time of log alignment. The reference time refers to the log time of the correlated feature. Then, determine the calibration time deviation

of each network device. The calibration time deviation refers to the deviation of log time of the correlated feature and the reference time. Finally, align the log time by subtracting the calibration time deviation from the log time of the network device.

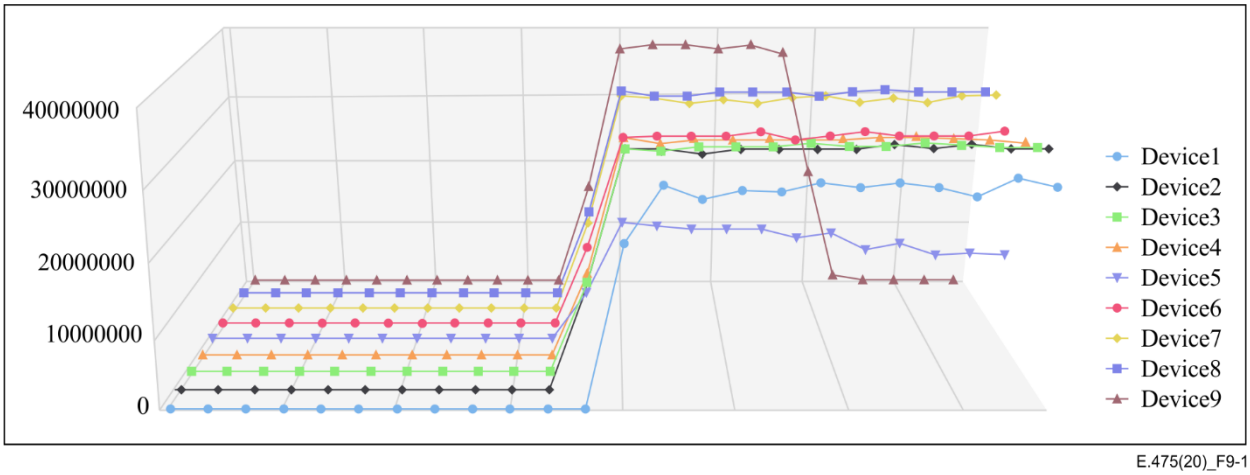


Figure 9-1 – Device logs relationship

9.1.1.2 Network log-based anomaly degree assessment

The procedure to assess log anomaly (as shown in Figure 9-2) has three steps.

- **Structured log construction**: Given a syslog file, construct a structured log by extracting keywords and match it to a log template that is learned from the existing log files. The log template matching can be done by:
  1) Classifying the logs into a set of categories with clustering algorithm [b-Mining-Clustering] or classification algorithm [b-Mining-Classification], e.g., classifying the logs based on module name or severity level.
  2) For the classified logs in each category, choose the first log as a template.
  3) Update the templates. For logs in each category, choose the second log to compare with the previous template: i) if there are existing variables, find out the positions of the variables, record these positions, and replace the variables in the template by wildcards. Update the previous template as the new one with wildcard(s); ii) if there are no variables, the previous template is not updated. Repeat this procedure until the last log comparison is completed, then get a final template with wildcard(s).
  4) Given a specific log in a set where logs are used to construct the template, find the category of the template to which it belongs.
  5) By comparing the above specific log with the template, the different parts on the log can be obtained and these differences can be identified as variables, and a structured log with variables of the specific log can be generated.
- **Feature engineering**: carry out pattern mining to extract features from the structured logs, which should comprise:
  – **Statistics of log event time series**: total number of log events; frequency of single log event per type.
  – **Event sequence patterns**: k-gram consecutive event sequence; rare co-appearing events mining; bursts of events.
  – **Log event type**
  – **Log severity level**

- **Log-based anomaly degree evaluation**: log's anomaly degree can be evaluated from a quantitative perspective as well as a perceived perspective. From a quantitative perspective, the number of the occurrences of suspicious patterns can be counted, including suspicious event patterns, events known to be results from network faults. From a perceived perspective, logs anomaly degree can be assessed by assuming that normal device logs exhibit similar patterns while anomalous ones do not. Hence by finding logs that are significantly different from other log files of the same type, such logs can be considered as suspicious.

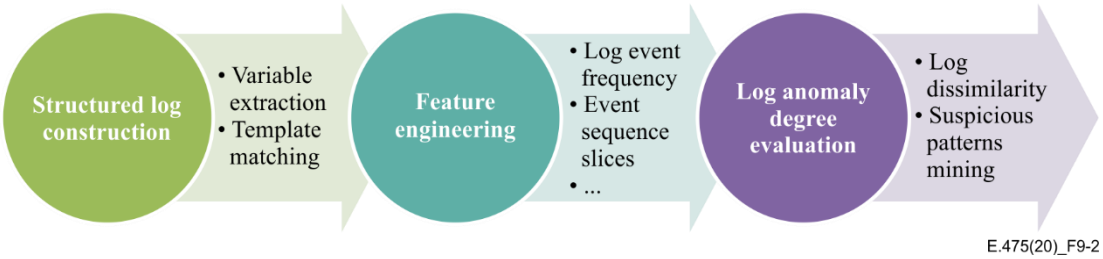


Figure 9-2 – Log anomaly degree evaluation model

9.1.2 Network KPI-based anomaly detection model

9.1.2.1 Network KPI-based analytics

Network KPI represents the operational state of a network device, link or network protocol in the network. One of the preconditions to guarantee the quality of service (QoS) of the network is the rapid and accurate detection of KPI anomalies. In general, the network KPI presents steady state changes with good network quality, while showing transient state change characteristics (e.g., burst change) when there is a network failure or abnormal state, which means the downgrading of network quality. Before anomaly detection, single or multiple KPI data of a network device should be collected for analysis, and each single KPI data refers to the values of the KPI measured at many collect time points.

Therefore, through the analysis of network KPI, two objectives can be achieved:

i) Identify the exact time point at which the network is abnormal and the associated KPI, which can help identify the causes of the failure, through the analysis of the historical data.

ii) Predict the future trend of the network KPI, in order to prevent and avoid the occurrence of failure by taking measurement results in the network abnormal stage, through the analysis of KPI during the current time period combined with the historical data characteristics.

9.1.2.2 Single KPI-based anomaly detection model

For network equipment performance anomalies, multiple features are usually extracted from KPI data, such as time, value, frequency, etc., and used as the key factors for anomaly analysis. It is necessary to use KPI-based anomaly detection tools to alert the equipment with KPI and take appropriate measures before the KPI-based anomaly gets worse.

This single KPI-based anomaly detection model does not rely on the manual preconfigured threshold to trigger an alarm. Instead, the KPI-based anomaly is automatically detected in advance and an alarm is triggered.

The procedure of the single KPI-based anomaly detection model is shown in Figure 9-3.

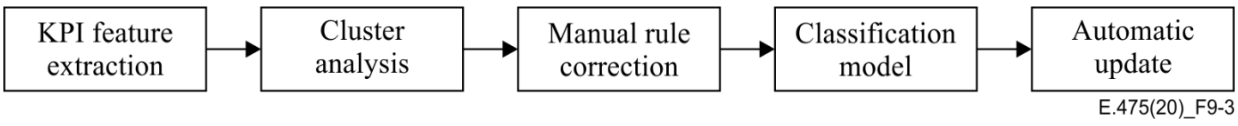


Figure 9-3 – Single KPI-based anomaly detection model

- **KPI feature extraction**. Slide time window and extract various features of a single KPI in the time window.
- **Cluster analysis**. Cluster analysis of statistical information in multiple time windows through a data mining clustering algorithm to identify and label anomalies segment at different level.
- **Manual rule correction**. Combine the cluster analysis results with the pre-configured manual rules to correct the clustering results.
- **Classification model**. Train the data with abnormal segment label at different level separately and establish classification model by using a classification algorithm. Check KPI-based anomaly by classification model. If any anomaly issue occurs consecutively, send a KPI-based anomaly alarm to the management system.
- **Automatic update**. Based on specific update rules, update training sets automatically and improve the accuracy of the classification algorithm.

9.1.2.3 Multi-KPI-based anomaly detection model

Generally, the number of network KPIs can be huge and they need to be analysed simultaneously. KPI data is collected based on KPIs, and the data of each KPI is decomposed into many data series. Those data series are collected from multiple network links or devices based on a single KPI and measured at many collection time points. Each data series includes many values measured at various collection time points, and these values are ranked in order of time.

This means that the analysed data is not a single KPI data series, but a multiple KPI time matrix with multiple data series, and each data series corresponds to one KPI. Through the matrix analysis method, the abnormal time point and the corresponding network KPI data series can be easily located from many data series. Thus, the abnormal KPIs can be determined based on the KPIs of the abnormal time point and/or data series.

The implementation of multi-KPI-based anomaly detection model is shown in Figure 9-4.

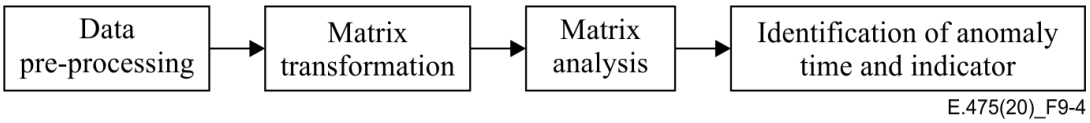


Figure 9-4 – Multi-KPI-based anomaly detection model

- **Data pre-processing**

  The multi-KPI data is decomposed to obtain the corresponding component sequences, e.g., the trend component sequence can be obtained if the Holt-Winters decomposition method is employed. Fourier decomposition is used to obtain the component sequence under certain frequency range. Then these data series are constructed as a trend matrix X ($X \in R^{M \times N}, M.N > 1$), each column of a matrix corresponds to a time series, and each row of a matrix corresponds to a collection time point.

  The column of the matrix can be normalized by the method of [0,1] normalization, logarithmic normalization, and so on. Alternatively, time series matrix normalization can be achieved by normalizing the original time series data and constructing these time series data into time matrix, instead of decomposing the time series.

- **Matrix transformation**

  The covariance matrix or similarity matrix is calculated using each column or row of the time matrix/trend matrix, and then the feature extraction is performed on Laplace matrix obtained from covariance matrix using convex optimization. The characteristics of the time matrix/trend matrix are those in which some vectors of the original matrix can be obtained by linear combination under matrix transformation method (e.g., Laplace transformation).

Generally, these feature extraction methods are typical singular value decomposition or feature decomposition methods.

- **Matrix analysis**

  Some features obtained by matrix transformation are used to construct the projection matrix, and the original data is multiplied by the projection matrix to perform the projection operation. Then the original data is projected into the feature space, or further reconstructed by the data in the feature space. Generally, the principal component analysis can be used to perform matrix analysis.

- **Identification of anomaly time and indicator**

  Initially, statistics can be calculated by the data projected in the feature space or the reconstructed data. Then, the threshold of statistics can be calculated by an empirical formula. If the statistical data is larger than the threshold, it is considered as abnormal data, and the corresponding time point and the KPI can be determined.

9.1.3 Network configuration detection model

9.1.3.1 Network configuration data analytics

When a network needs a setup, repair, modification, expansion or upgrading, the administrator needs to deploy a large number of configuration files on network devices. A misconfigured network device can have a disastrous impact on network connectivity and network performance, which may cause the waste of tremendous network resources and modification of network topology since network service deployments are often coupled to network topology. It is therefore important to check configuration files on a regular basis in order to avoid mismatches or incompatibility issues.

Since configuration files change only upon the network setup, repair or upgrading, it is sufficient to carry out examination offline. It is advised to schedule a regular backup of configuration files on all devices. Configuration files are vendor-specific and in plain text format, which can be stored in separated storage systems.

9.1.3.2 Network configuration faults detection model

Automatic configuration faults detection requires the following three steps as shown in Figure 9-5:

1) Template generation: given a set of configuration files, use keyword extraction techniques to transform them into structured templates.
2) Network role match: compare the structured template with the typical network role's template regarding each device's role. A network role describes the device's functionality in a network.
3) Configuration comparison: a configuration file is considered as anomalous if the template is different from the template with its pre-defined role in a network. Network role template extraction can be built offline with clustering methods.

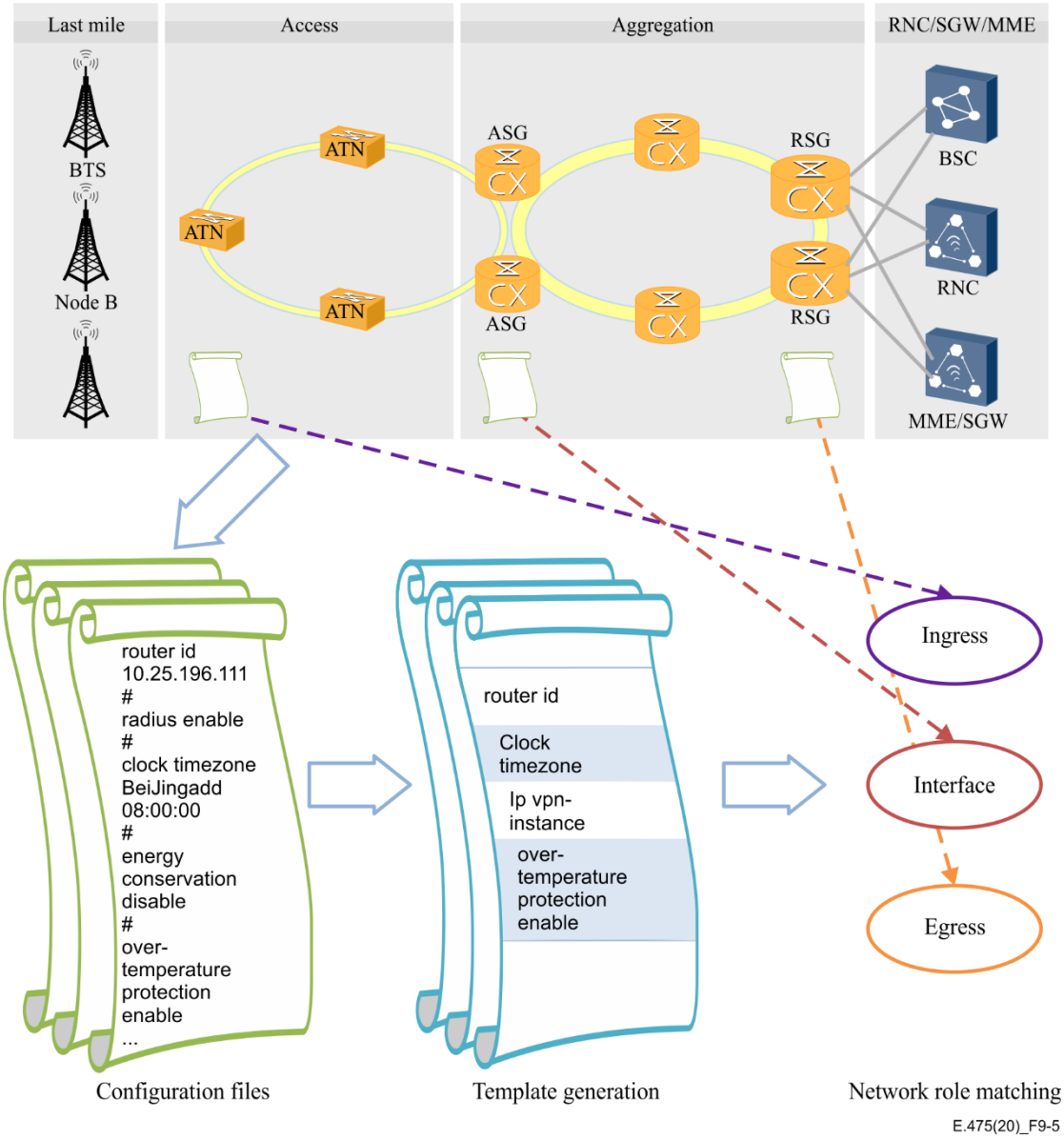


Figure 9-5 – Configuration anomaly detection model

9.1.4 Root cause diagnostics model

The ultimate goal of this Recommendation is to help network administrators focus on dimension issues and provide solution strategy suggestions for them to take timely actions when network problems occur. The root cause diagnostics model is designed to achieve such goal.

It is very challenging to identify root causes of network problems because of complex symptoms of network issues. Many network issues exhibit similar symptoms and may cause cascading failures, which may result in generating a large number of warnings or trouble tickets. Hence, associating the observed symptoms with possible root causes require network-specific knowledge and experience. When there is a fault in the network, it is critical to dimension the issue and take prompt actions in order to mitigate its impact on a larger network performance area. Hence, a quick analysis of potential root causes and provision of the corresponding solution strategies can be a great help that can assist administrators to make timely decisions when network problems occur.

9.1.4.1 Root cause data analytics

Data source collecting procedure

The input data of root cause diagnostics tools include human descriptions that point out the problematic devices as well as human perceived network problems. The tool will process these descriptions to target suspicious devices. It will then retrieve the log files, KPI and configuration files of the targets and try to detect anomaly with these data sources.

Root cause ranking and solution strategy recommendation

To identify the root cause of network problems, a database can be maintained, including expertise such as an anomaly-fault matching table (as shown in Table 9-1) and the fault trees. Besides the built-in database that contains such domain knowledge provided directly by network experts, more rules can automatically be incrementally built with information history via machine learning techniques.

Table 9-1 – Anomaly-fault matching table

Anomaly	Fault
OSPF_Nbr_UP/OSPF_Nbr_Down occur frequently	Router flapping
The types of two network elements' configurations are different	Configuration inconsistency

9.1.4.2 Root cause diagnostics

Root cause diagnosis consists of three steps (as shown in Figure 9-6):

1) Extract the anomaly by administrators' description and the log files, KPI and configuration files of the suspicious devices.
2) Map the anomaly to network faults according to the anomaly-fault matching table, which describes the casual relationships between symptoms of anomaly and network faults.
3) Traverse fault trees with extracted faults and find out the root cause candidates.

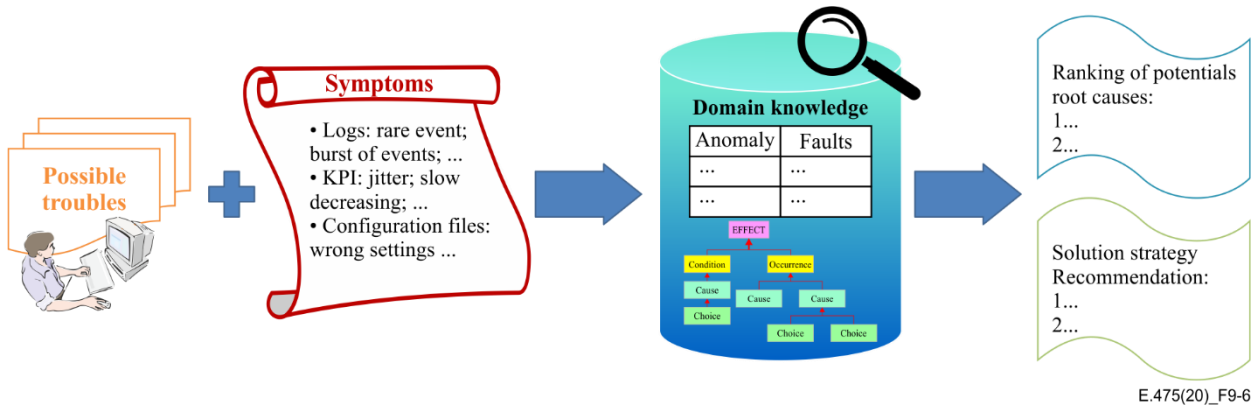


Figure 9-6 – Root cause diagnostic model

9.2 Network risk assessment models

9.2.1 Network KPI based risk evaluation model

9.2.1.1 Network KPIs analytics

Network KPIs provide fine-grained understanding of network performance, which bring more value to network maintenance and operation, including identification of possible bottlenecks, dimensioning issues, and locating the need to perform network optimization. The ability to properly handle the large amount of noisy KPI data is vital to gain these desired insights. This clause describes methods and practices of data-handling techniques and methodologies for using network KPIs data for network risk evaluation.

Out of the large amount of available KPIs, a few that represent the most common and practical KPIs can be selected. The common usage of these KPIs can be classified into the following three categories:

- Device availability and device risk: Device availability can be measured with packet loss. Most network devices use local features (CPU/memory/temperature) to monitor their own risk.
- Network interface statistics: inbound and outbound statistics including traffic, errors and packet discards per interface.
- Network link statistics: Link statistics tell what is occurring on the link itself versus device and interface statistics, which tell what is happening on the device. In the case of the wavelength division multiplexing (WDM) network, typical KPIs include FEC_bef (Forward Error Correction coding before error correction), FEC_aft (Forward Error Correction coding after error correction), input optical power, output optical power, etc.

9.2.1.2 Risk assessment

Given hundreds of thousands of KPI data, how to measure the network quality and provide network risk assessment is a challenging issue. A good network risk assessment criteria should be indicative of local network-level problems, and hence be able to provide prompt warnings and help locate potential problems when trivial but persisting anomalies are observed. Meanwhile, the system performance should be described in a global sense by aggregating multi-faceted information with large number of KPIs across the network infrastructure. Designing such a KPI network risk criterion presents the following challenges:

1) Single KPI-based scoring: the scoring strategy for single KPI.
2) Multi-KPI-based scoring: the scoring strategy for assessing the network risk using the values of many KPIs.

1) Single KPI-based scoring

For network problems, traditional solutions are based on alarming and the problems are often tackled after service interruption, which would result in ineffectiveness and lead to prolong service interruption. In this clause, several dimensions of a KPI are examined, such as fluctuation, trend and characteristic. Additive models are used to integrate variations, threshold values together with trends of KPI values in the scoring strategy, as shown in Figure 9-7. After time series KPI data is pre-processed, three different dimensions of a KPI are analysed, and an evaluation process is used to assign different weights for these dimensions and score the single KPI.

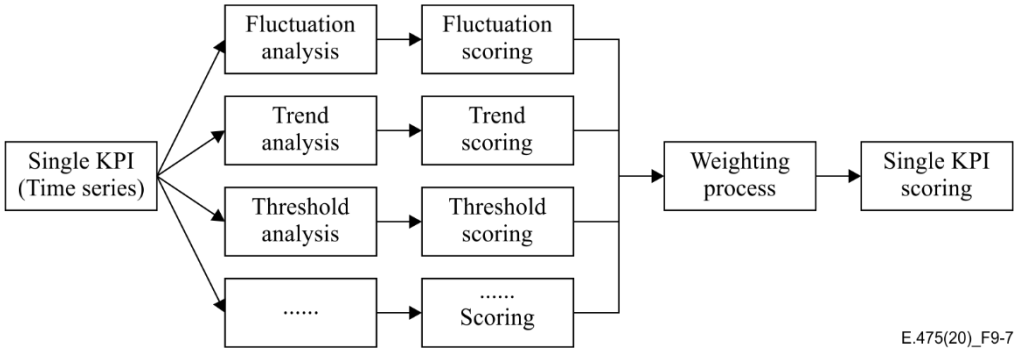


Figure 9-7 – Single KPI-based scoring strategy

a) Fluctuation analysis

For the time series KPI data within a time window A (e.g., 10 days), the outliers and noise in the KPI data are first removed. In the normal situation, the individual KPI should always be maintained close to a constant value which is regarded as the steady-state value. The steady-state value of the KPI can be set as a benchmark value for further comparison. Generally, the steady-state value can be calculated by the average of all KPI data within the time window A.

Then, the fluctuation distance between the KPI data and steady-state value is calculated within a time window B (e.g., 4 hours) in real time via formula (1). Here the end time of time window B should be larger than or equal to the end time of time window A.

Finally, based on the fluctuation distance, the fluctuation score can be calculated via formula (2). The fluctuation score is used to indicate the fluctuation. The bigger the fluctuation score, the higher the severity level of the fluctuation.

Noise and abnormal data can have side effects on time series KPI data when estimating the steady-state values of KPIs based on these series. It is critical to remove the outlier data and suppress the impact of noises before analysis. To remove the outliers, a three-sigma rule can be applied for KPIs that follow normal distribution. Next, the principal component analysis (PCA) [b-PCA] can be used to reduce the noise impact on the time series KPI data. The underlying idea is that the observed KPI value can be decomposed as a normal component and an abnormal component. The former shows normal traffic patterns, which lies in a very low-dimensional subspace and can be separated using PCA.

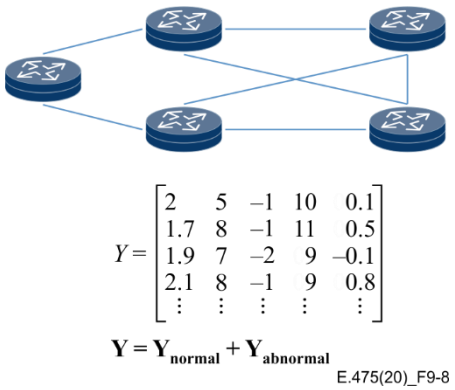


Figure 9-8 – Noise suppression

Take FEC_bef for example, it can be seen as a single KPI. Let $X_i,\ i = 1, \dots, N$ being the KPI data within time window B, with μ the steady-state value, then the fluctuation distance can be computed by common statistical calculations, such as mean, variation coefficient and standard deviation. Here the method of standard deviation is provided as an example. The fluctuation distance can be obtained by:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \mu)^2} \tag{1}$$

Then, the fluctuation score of x can be calculated as:

$$S_{deviationdist} = \begin{cases} 0 \le \sigma \le b, & (100 - \frac{100}{b}) \cdot \sigma \\ \sigma > b, & 0 \end{cases} \tag{2}$$

where b is the user-specified parameter and is usually set to 2 according to user experience.

b) Trend analysis

In this clause, the exponentially weighted moving average (EWMA) [b-EWMA] is employed for trend analysis of time series data within a time window C (e.g., 30 days). Here the last time of window C should be less than or equal to the last time of window B. EWMA is used for smoothing the ranked KPI data like the other moving averages. In this method, weights are applied to the data such that time points further in the past will receive less weight (and therefore be less impactful on the result) than more recent time points. This applies a non-uniform weighting to KPI data, so that a lot of data can be used, but recent data is weighted more heavily. As the name suggests, weights are based upon the exponential function. By decomposing the KPI data, trend component can be obtained.

After EWMA, linear fit is implemented to calculate the deterioration of trend component within such time window. With k representing the deterioration value, the trend score can be calculated as:

$$S_{trend} = \begin{cases} 0, & k < -3 \\ \frac{100}{3} \cdot (x + 3), & -3 \le k \le 0, \\ 100, & k > 0 \end{cases} \tag{3}$$

Note that the trend score is used to represent the change of KPI value (i.e., ascend or descend) as well as the change speed of such value.

c) Threshold analysis

For each network device, a KPI threshold is defined to support at the maximum level. Take time window B as example again, the KPI data value at the end time of time window B is used. When this value is higher than the KPI threshold, the closer the two values are, the lower reliability the KPI value is. When this value is smaller than the threshold, the corresponding deviation score is 0.

In the case of FEC_bef KPI, and if $x \in R$ is the value of KPI data, the deviation score can be calculated as:

$$S_{threshdist} = \begin{cases} 0, & x \geq \gamma \\ 100 \cdot \left(\frac{\gamma - x}{\gamma - x_{min}}\right), & x < \gamma \end{cases}, \quad (4)$$

where γ is the FEC_bef threshold, which is determined by hardware property of the device, x_{min} is the minimum value within the time window.

d) Evaluation process

After three dimensions of a KPI are analysed, the corresponding scores are calculated. The main goal of the evaluation process is to assign different weights of three dimensions, e.g., 0.2 to fluctuation, 0.3 to trend, and 0.5 to threshold. Then, the score of a single KPI can be calculated as:

$$S_{BEFScore}(x) = w_1 \cdot S_{deviationdist} + w_2 \cdot S_{trend} + w_3 \cdot S_{threshdist} \quad (5)$$

where w_1, w_2, w_3 are weights of fluctuation, trend and threshold respectively.

According to the devices' documentary, the states of the devices' working condition can be mapped directly to KPI value ranges. By leveraging such domain knowledge, the range threshold values can be integrated into the scoring strategy. As mentioned above, the single KPI-based scores are valuable for analysing potential big network-level problems. For example, when the KPI-based score is higher than 80, the device has a high probability of failure; when it is lower than 30, the device has a high probability of safety and when it is within the range of [30, 80], the status of the device is sub-health.

2) Multi-KPI-based scoring

Based on the various monitor mechanisms, if any high risk occurs in the network, administrators can be informed at a very early stage. If a device or a service is monitored by several key KPIs, the risk should be analysed by the integration of these KPI-based scores. That is, the reliability score of this device or service is calculated by many weighted KPI-based scores, as shown in Figure 9-9.

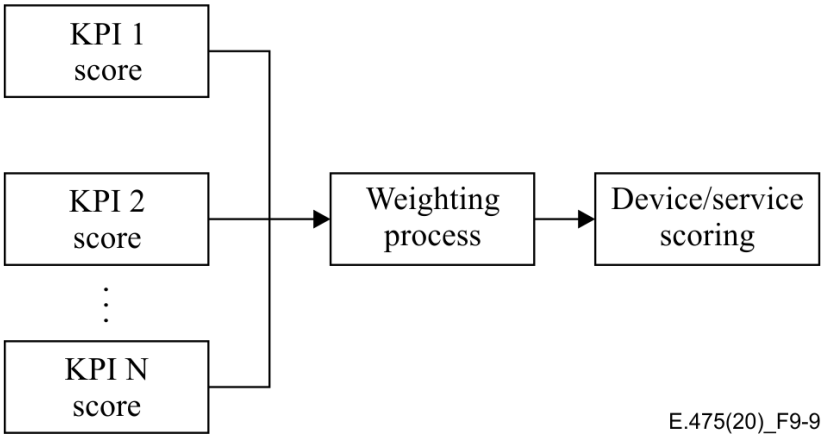


Figure 9-9 – Multi-KPI-based scoring strategy

Take wavelength division service, for example, its quality is determined by two key KPIs: FEC_bef (FEC coding before error correction) and FEC_aft (FEC coding after error correction). These KPIs are monitored and the corresponding scores are used to analyse the reliability of wavelength division service quality. Therefore, the score of wavelength division service can be calculated as:

$$S_{FEC}(x) = w_4 \cdot S_{BEFScore} + w_5 \cdot S_{AFTScore} \quad (6)$$

where $S_{AFTScore}$ is the score of FEC_aft KPI, and w_4, w_5 are weights of two KPIs, respectively.

9.2.2 KQI-KPI based risk evaluation model

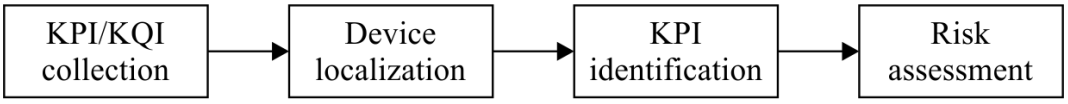
9.2.2.1 KQI-KPI-based data analytics

Operators are increasingly concerned about the user experience, network bottlenecks/risks that need to be identified and optimized before network failures and bad user experiences. However, due to the lack of effective means, it is hard to identify network bottlenecks in advance.

Network risks are traditionally evaluated by KPIs alone, such as delay, jitter, and packet loss. However, good KPI does not necessarily imply good service quality, because KPI alone is insufficient to forecast the degrading of service quality and end-users' QoE. Hence, it is important to identify useful key quality indicator (KQI) to evaluate end-users' experiences and build the association between KPI and KQI, e.g., collect data from various data sources in a holistic manner in real time, which will then be condensed into KQIs that indicate the realistic users' QoE. Processing the enormous amounts of data generated by video services in real time can be very challenging. The processing task can be accomplished by leveraging big-data processing systems such as Apache Kafka and Apache Spark Streaming.

9.2.2.2 KQI-KPI-based risk evaluation

The goal of KQI-KPI-based risk evaluation analysis is to use a model to identify which lower level KPI on device affects KQI. The KQI-KPI-based risk evaluation model is shown in Figure 9-10.



E.475(20)_F9-10

Figure 9-10 – KQI-KPI-based risk evaluation model

1) KPI/KQI collection

KPI and KQI data can both be collected on network devices. It is important to choose the appropriate KPI indicators and KQI parameters for correlation analysis. The collected KPI data of network devices include port occupancy rates, port queue packet lost ratio, port optic power, CRC packet lost ratio, etc. The collected KQI data can be the quality of the pictures (voice & video), zapping time (channel change latency), response time of request.

2) Device localization

Firstly, very annoyed person (VAP) are identified based on KQI indicators, such as video freezing duration time. VAP refers to a customer who has extremely poor service experience but has not complained to the customer services centre as yet and has a high probability of churning.

Then, the degrading network device can be identified based on the resource management data and network topology.

3) KPI identification

When KPI and very degrading network device are both available, the next step is to correlate the degrading network device with KPI. All device-related KPIs are analysed, and the key KPIs which influence the performance of device are identified.

4) Risk assessment

In this phase, a network KPI based risk evaluation model (clause 9.2.1.2) can be used to assess the potential network risk.

Appendix I

Network analytics and diagnostics applications

(This appendix does not form an integral part of this Recommendation.)

This appendix provides various network analytics and applications and gives some examples.

I.1 Causes of network performance degradations

Fault source: When the end-to-end latency increases or throughput goes down, the fault is usually attributed to the network, which leads to resource waste and longer fault diagnosis. The network anomaly degree indicator can be used to judge whether the network is responsible for the fault. If the problem is caused by other factors (e.g., encoding/decoding issue, bit rate issue, interaction between application and the transport), the network is not the source of network performance degradations.

It is not easy to determine if the quality degradation is caused by the network. To determine whether the performance degradation is caused by the network, the evaluation of the network anomaly degree or the condition of network SLA condition can be performed with the key performance metrics such as network latency and packet drop rate.

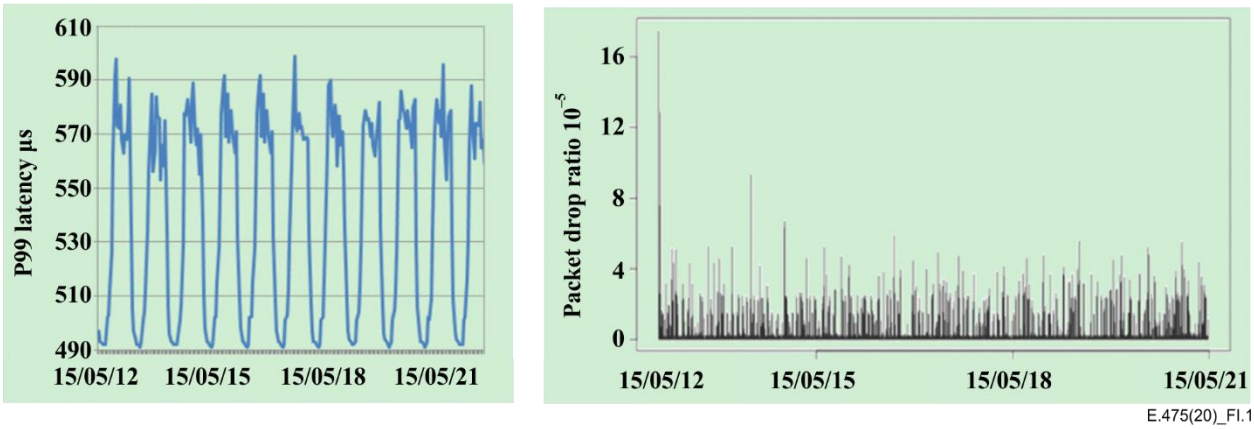


Figure I.1 – An example of fault source determination

Evaluation procedure:

- Network probe detects the network performance degradation and report it to the data collection model of the INAD.
- After the data collection model gathers the network SLA data, it determines the causes of network performance degradation using a real time network anomaly assessment system.
- If the network SLA is acceptable, the network is not the source of the performance degradation.
- If the network SLA is not acceptable then the network is the source of the performance degradation.
- If the network is the source of the performance degradation, then find the location and type of the performance degradation in the network based on the analysis of the correlation between the network topology and data.

I.2 Network health indication

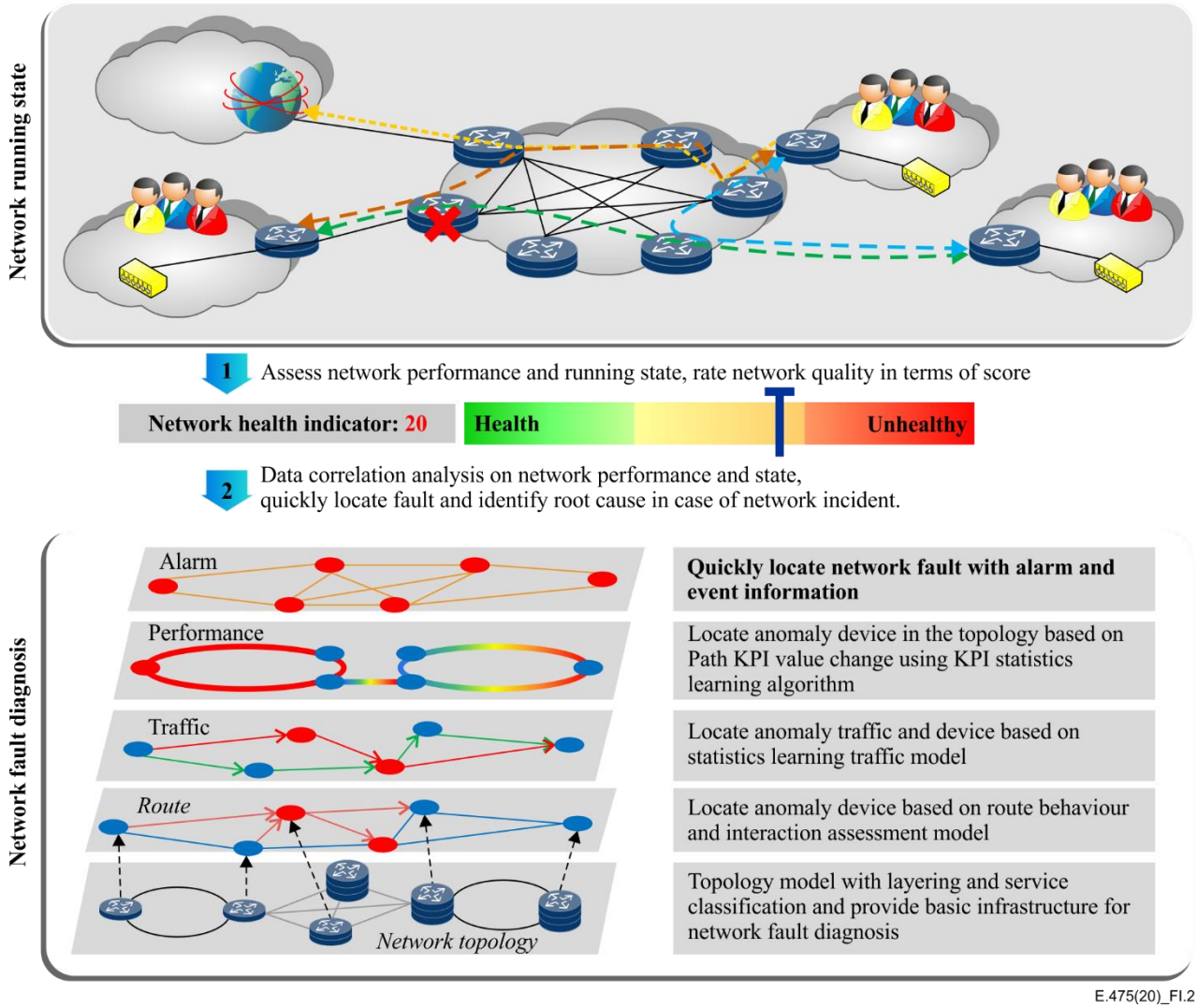


Figure I.2 – An example of network health indication

Before the network diagnosis is performed, the evaluation of the network performance and health degree, and rating of the network health degree in terms of score are performed.

In this case, the network health degree is expressed as an integer in the range [0, 100]. As an example, the range [0, 30] indicates that the network is healthy and the range (80, 100] that the network is unhealthy. A threshold value in the range (30, 80] is set as 80, if and only if the network health degree exceeds the threshold value 80, then the network diagnosis will be triggered in the network.

I.3 Prediction of network performance degradations

The objective of this use case is to quickly identify the causes of the network performance degradation and also to predict forthcoming situations, take action to repair recognized situations and to recover from network performance degradation.

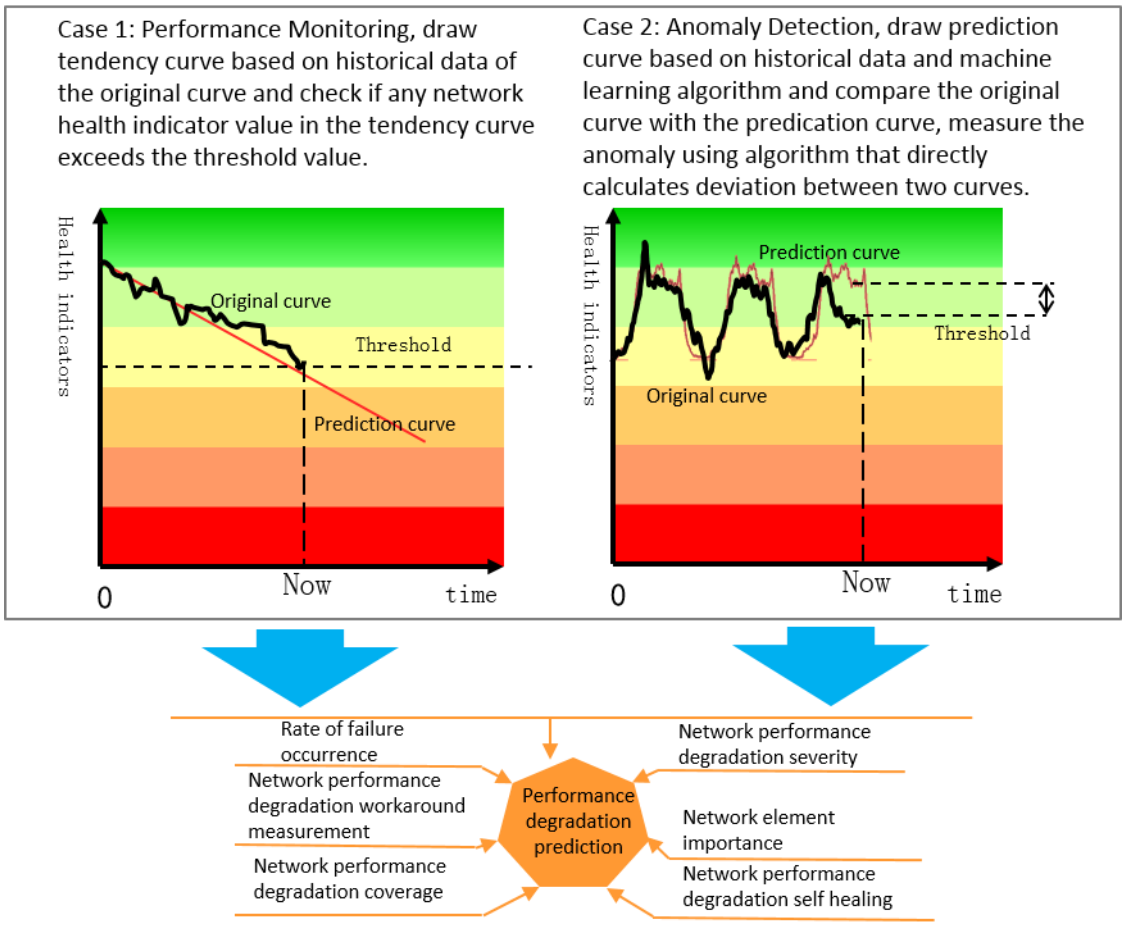


Figure I.3 – An example of prediction of network performance degradation

There are two possible cases for network performance prediction:

Case 1: The black curve reflects the current network anomaly status before the time point now, the red curve is a tendency curve extracted from the historical data in the black curve, and an alert will be raised when the tendency curve exceeds the threshold line.

Case 2: The black curve is the same as for case 1, the red curve is a predication curve based on a prediction algorithm and historical data in the black curve. The deviation value between two curves at any time will be compared with a differential threshold. If it exceeds the threshold, then an alert will be triggered to report the anomaly to the diagnostic module of the INAD.

I.4 Memory anomaly detection

In general, anomalies in the network equipment memory, which could be manifested as corrupted event records in the logs, high memory usage or even memory leakage, may lead to malfunctioning of the network equipment and network down time. For example, in an SDN environment, the SDN controller stores the whole network information in its memory. Memory leaks and other anomalies are sufficient to cause the controller to crash, which results in network failure. In addition, security problems such as continuous allocation of memory space leading to memory leak may cause systems to suddenly quit the process.

This clause illustrates an example of the single KPI anomaly detection model (described in clause 9.1.2.2) to perform memory anomaly detection, as shown in Figure I.4.

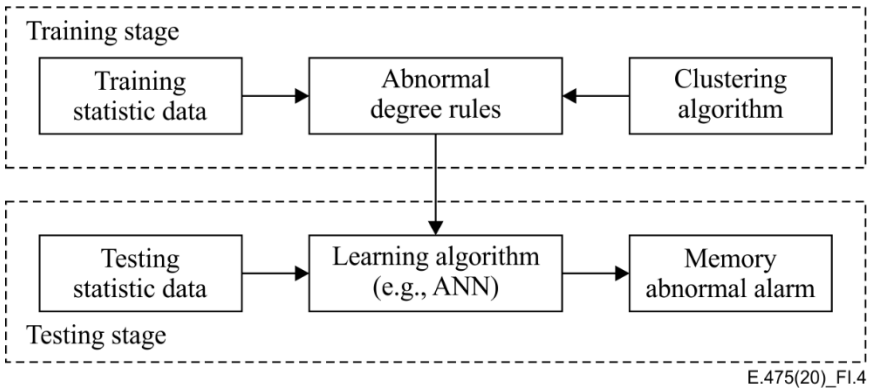


Figure I.4 – An example memory anomaly detection

I.4.1 Training stage

At the training stage, the training memory log consists of log data collected through multiple garbage collections. The log data of each garbage collection includes garbage collection time and at least one of the following information: downtime, memory occupancy rate after garbage collection and memory occupancy rate before garbage collection. Log data in this time window refers to the log in the time window to which garbage collection time belongs. For many training time windows, training statistic data can be constructed by log data in any time window. Training statistic data includes at least one of the following information: the average downtime, the memory occupancy rate change between the memory occupancy rate before the earliest garbage collection and the memory occupancy rate after the latest garbage collection, and memory occupancy rate after the latest garbage collection within any time window. However, the number of garbage collections should be included in the training statistic data.

Then, the training statistic data is clustered into at least two categories by a clustering algorithm [b-IEEE Clustering]. The abnormal degree of training statistic data in each category is determined by computing the average of the key attribute, which is one of attributes in the training statistic data.

The abnormal degree of each training time window can be determined by the abnormal degree of the training statistic data within the training time window.

Moreover, rules of abnormal degree can be determined based on the training statistic data and the abnormal degree of training time window. After that the rules are exported to the next testing stage to determine the abnormal degree of the memory.

I.4.2 Testing stage

At the testing stage, testing memory log consists of log data collected through multiple garbage collections. The log data of each garbage collection includes garbage collection time and at least one of the following information: downtime, memory occupancy rate after garbage collection and memory occupancy rate before garbage collection. Testing statistic data can be constructed by integrating log data within the testing time window of the memory log. Such testing time window refers to the time window which garbage collection time belongs to. Testing statistic data includes at least one of the following information: the average downtime, the memory occupancy rate change between the memory occupancy rate before the earliest garbage collection and the memory occupancy rate after the latest garbage collection, and memory occupancy rate after the latest garbage collection within the time window.

Then, the abnormal degree of log data within the testing time window can be determined based on the comparison between the testing statistic data and the corresponding rules. The rules are computed in advance based on garbage collection time and/or downtime and/or memory occupancy rate before garbage collection and/or memory occupancy rate after garbage collection in the training memory log.

After the abnormal degree is determined, the log can be classified into several clusters, such as normal log and abnormal log. In the case of abnormal log, if memory occupancy rate after garbage collection is smaller than the preconfigured value, and downtime is smaller than the preconfigured downtime, the abnormal log can be considered as a normal log.

Note that the number of garbage collections should be included in the testing statistic data. If abnormal log consecutively occurs more than preconfigured times, a memory abnormal alarm is raised.

I.5 Network fault localization

With the rapid development of the network video industry, for example, the emergence of Internet protocol television (IPTV) services and over the top (OTT) services, operators have gradually shifted their focus from network coverage and network quality assurance to "user-centric" operations, especially focusing on the user experience. The quality of the user experience is directly related to the user market share and improving the video user experience can further promote business growth. In an IPTV system, if a network device or link fails, such as port, subcard, and board of the device, the IPTV users will be directly influenced. Therefore, when a network device breaks down and the user experience deteriorates, the INAD needs to locate the faulty device timely and accurately in order to fix the fault promptly to ensure a better user experience.

This clause illustrates an example of single KQI-KPI based risk evaluation model (described in clause 9.2.1) to perform network device fault localization, as shown in Figure I.5. Three decisions are made to recognize the faulted devices, with the sequence of probable faulted devices, highly probable faulted devices and faulted devices.

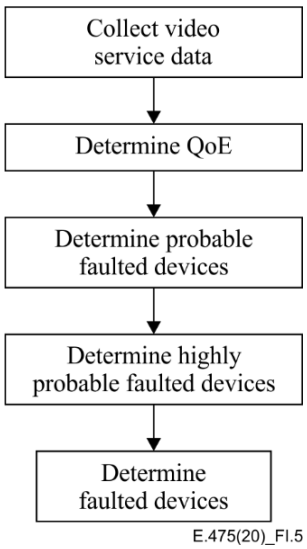


Figure I.5 – An example of network device fault localization

1) Collect video service data

In the case of video services, the video service data is collected at the first step. It includes experience data, network topology data, and resource management data. Network topology data is used to represent a connection relationship or service path between the network devices. The service path is used to represent a connection over which the service traffic streaming is transmitted. The resource management data is used to represent a connection relationship between a user device (e.g., STB) and a network device (e.g., ONT). User experience data includes at least one of the following features: video quality (e.g., vMOS), stalling duration, stalling proportion, stalling frequency, blockiness frequency, blockiness duration, blockiness proportion, blockiness times, blockiness area proportion, video quality switch times and poor quality proportion of video quality.

2) Determine QoE

According to the network topology data and resource management data collected in step (1), all the user devices served by the network device can be identified and QoE can be determined by the user experience data on the user devices.

3) Determine probable faulted devices

Assuming higher values indicate better quality, a threshold is set to the previously determined QoE values to identify an initial set of probably faulted devices whose QoE values are less than the threshold.

4) Determine highly probable faulted devices

For a probable faulted device, put it with other network devices which have common one-hop upstream network device with the possible faulted device into a set, e.g., set A.

For all network devices in set A, analyse the distribution of their QoE values. Based on the skewness of the distribution, the network devices with outlier QoE values can be determined as highly probable faulted devices.

5) Determine faulted devices

Once the highly probable faulted device has been identified, put its one-hop downstream network devices into another set, e.g., set B. Clustering QoE values of the downstream network devices in set B.

Compute the ratio of the number of the downstream network devices with low QoE values to the total number of all downstream network devices.

$$P_s = \frac{Q_{max}}{Q_{all}} \tag{I.1}$$

Q_{max} is the max number of the downstream network devices with low QoE values, and Q_{all} denotes the total number of all downstream network devices. P_s is the ratio of the above two numbers.

When P_s is bigger than the pre-set threshold, the corresponding highly probable faulted device is determined as a faulted device. Note that all the thresholds are set by the operators depending on their own service policies, and are not compelled to be same to all operators.

Bibliography

[b-ITU-T E- Sup.10] ITU-T E.800 series Recommendations Supplement 10 (2016), *QoS/QoE framework for the transition from network oriented to service oriented operations*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[b-ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.

[b-IEEE Clustering] The 3rd IEEE Workshop, *A Data Clustering Algorithm for Mining Patterns From Event Logs*, 2003.

[b-EWMA] NIST/SEMATECH e-Handbook of Statistical Methods: *EWMA Control Charts at the National Institute of Standards and Technology*.

[b-keyword-Extraction] Beliga, Slobodan; Ana, Meštrović; Martinčić-Ipšić, Sanda. *An Overview of Graph-Based Keyword Extraction Methods and Approaches*. // Journal of Information and Organizational Sciences. 39 (2015), 1; 1-20.

[b-Mining-Classification] R. O. Duda, P. E. Hart, and D. G. Stork. *Pattern Classification*. John Wiley & Sons, USA, 2nd, edition, 2001.

[b-Mining-Clustering] R. Xu and D. Wunsch, *Survey of clustering algorithms*, IEEE Trans. Neural Networks, no. Vol.16, Issue 3, pp. 645-678, May 2005.

[b-NLP] Journal of Machine Learning Research 2493-2537, *Natural Language Processing (Almost) from Scratch*, 2011.

[b-PCA] Wold, S., Esbensen, K., & Geladi, P. (1987). *Principal component analysis*. Chemometrics and Intelligent Laboratory Systems 2 (1 /3), 37/52.

[b-RFC5424] IETF RFC 5424 (2009), *The Syslog Protocol*, March.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	**Overall network operation, telephone service, service operation and human factors**
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020