ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3184 (05/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Mechanism for intelligent awareness of network status

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	**Y.3000-Y.3499**
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

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

Recommendation ITU-T Y.3184

Mechanism for intelligent awareness of network status

Summary

Recommendation ITU-T Y.3184 specifies a mechanism for intelligent awareness of network status. The scope of this Recommendation includes: introduction of intelligent awareness of network status; overview of the mechanism for intelligent awareness of network status; mechanism for intelligent awareness of network fault; mechanism for intelligent awareness of network performance; mechanism for intelligent awareness of network resource; mechanism for intelligent awareness of network load; and mechanism for intelligent awareness of other aspects of network status and security consideration.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3184	2023-05-14	13	11.1002/1000/15534

Keywords

Intelligence awareness, mechanism, network status.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T Y.3184

Mechanism for intelligent awareness of network status

1 Scope

This Recommendation specifies mechanism for intelligent awareness of network status. The scope of this Recommendation includes:

a) Introduction of intelligent awareness of network status;

b) Overview of a mechanism for intelligent awareness of network status;

c) Mechanism for intelligent awareness of network fault;

d) Mechanism for intelligent awareness of network performance;

e) Mechanism for intelligent awareness of network resource;

f) Mechanism for intelligent awareness of network load;

g) Mechanism for intelligent awareness of other aspects of network status;

h) Security consideration.

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.

[ITU-T F.747.10] Recommendation ITU-T F.747.10 (2022), *Requirements of distributed ledger systems for secure human factor services.*

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

[ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*

[ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection*

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

[ITU-T Y.3601] Recommendation ITU-T Y.3601 (2018), *Big data – Framework and requirements for data exchange*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 network status awareness: The technologies and methods that make various network roles such as network builder, network operator, network service provider and network user aware of the network status, such as network resource, network performance, network fault status and other network status.

3.2.2 intelligent awareness of network status: Technologies and methods of network status awareness that are enhanced by artificial intelligence and machine learning.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS	Business Support System
CPU	Central Processing Unit
DFI	Deep Flow Inspection
DPI	Deep Packet Inspection
EMS	Element Management System
ETL	Extracting Transformation Loading
NMS	Network Management System
OSS	Operation Support System
RF	Radio Frequency

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Introduction of intelligent awareness of network status

Network status awareness is a kind of technology and method that makes various network roles such as network builder, network operator, network service provider and network user aware of the network status, which includes network fault status, network performance status, network resource status and other network status, in a timely manner. Higher and higher requirements about the awareness of the network status are being brought forward by future networks so that the network can be operated and managed more efficiently.

Artificial intelligence and machine learning related technologies can be used in various network areas including network planning, network re-structuring, network optimization and so on. It is likely that artificial intelligence and machine learning related technologies can also help to improve the function and performance of network status awareness.

While injecting network status awareness with artificial intelligence and machine learning related technologies, network status awareness will evolve to a new technology branch called intelligent awareness of network status.

Comparing the intelligent awareness of network status with traditional network status awareness, several main differences can be found, as follows:

- Traditional network status awareness collects network status data from the network directly, while intelligent awareness of network status not only collects direct network status data but also achieves new network status data from direct network status data.
- Traditional network status awareness only takes the network status data into account while intelligent awareness of network status will additionally take other factors such as time, environment and network history information into account.
- Traditional network status awareness only reports network status data to the network operator and network service provider, and intelligent awareness of network status will analyse network status data, dig internal law from the network status data and give some possible proposals to the network operator and network service provider in order that they can reconfigure and restructure the network based on received network status data.

7 Overview of mechanism for intelligent awareness of network status

7.1 General model for intelligent awareness of network status

Generally, intelligent awareness of network status is the capability that the network status is intelligently understood and grasped by the network owner or the network operator based on information collected from the network. Network status is the situation information when the network is running, and it can be described by some network status index. Generally, not direct network status data but intelligent network status information is the final output of the function for intelligent awareness of network status. For example, if the direct network status data is that data transport is interrupted, the final intelligent network status can be that the interface is out of order, the software system of the network device does not work or the optical fibre that connects the interfaces is cut off, etc.

Figure 7-1 describes a typical model for the intelligent awareness of network status. It shows four main parts of intelligent awareness of network status.

- Network: this represents the network data plane or infrastructure of the network.
- Network status sensing: this aims to collect basic status data from the network and transform basic status data to simple status information that can be easily understood and handled by succeeding functional entity.
- Network status analysing: this is to transform simple network status information to intelligent network status information.

  NOTE – Basic network status data is the data that can be collected from the network directly; in other words, basic network status data can be also called network direct status data. Simple status information is some information transformed from basic status data. Intelligent status information is the information that can be achieved through analysis of the simple status information. It is not required but recommended to transform basic network status data to simple network status data in order that network status analysis function can process the data more easily. Under some circumstances, basic network status data can also be thought of as simple network status data if it can be easily understood by succeeding functional entity and transformation is not required.
- Network status reporting and displaying: this realizes the function to report intelligent network status information and take some action to fix possible network problems and improve the network status.

The four parts are basic components of the model and the four parts are responsible for status data generating, simple network status information sensing, intelligent status information generating and intelligent status reports, respectively.

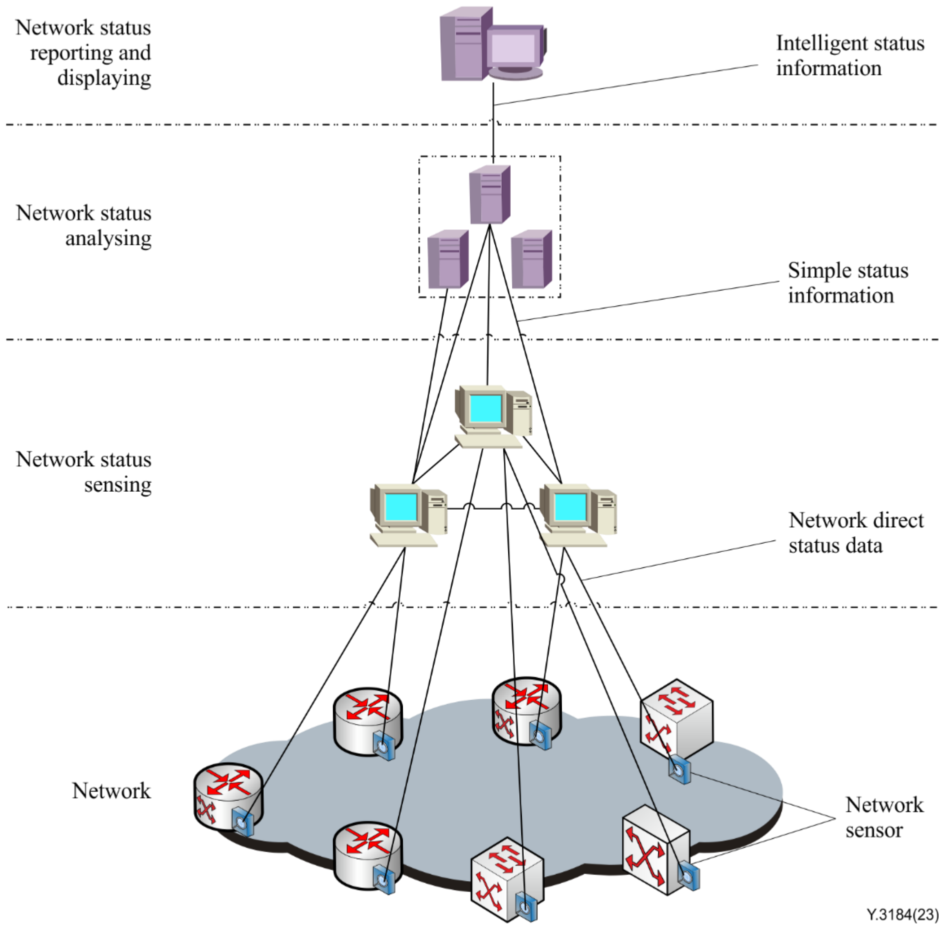

Figure 7-1 – A typical model for intelligent awareness of network status

7.2 General procedure for intelligent awareness of network status

Figure 7-2 depicts a general process for intelligent awareness of network status, and the following procedures are shown:

- Generating basic network status data.
- Collecting basic network status data.
- Transforming basic network status data into simple network status data.
- Intelligently analysing simple network status data.
- Generating intelligent network status information.
- Taking the action based on the intelligent network status information.

It should be emphasized that the most important procedure is analysing simple network status information intelligently. However, it is sure that every procedure is required.

Many methods can be used in the aforementioned procedures. For example, deep packet inspection (DPI), as described in [ITU-T Y.2770] and [ITU-T Y.2771] can be used to collect basic network status data. Data pre-processing methods, such as extracting, transforming and loading (ETL) as described in [ITU-T Y.3600] and [ITU-T Y.3601], can be used to transform basic network status data into simple network status data. It is noted there are also many methods or technologies that can be used to implement the function to analyse simple network status information intelligently (see clause 7.3).

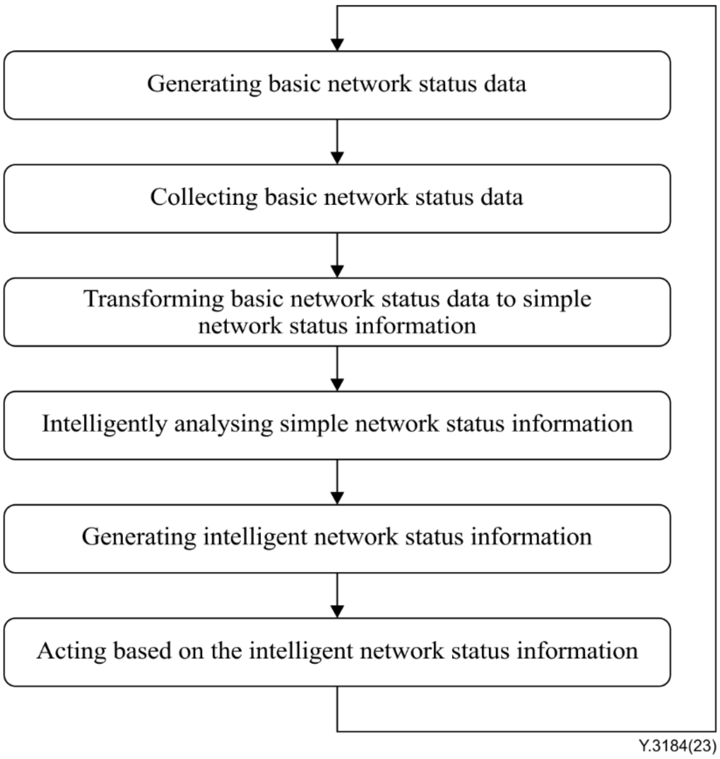

Figure 7-2 – General process for intelligent awareness of network status

7.3 The main methods for intelligent awareness of network status

There are a lot of methods that are helpful to intelligent awareness of network status, and those methods include but are limited to the following classes:

- Classification analysis of simple network status data.
- Cluster analysis for simple network status data.
- Correlation analysis of simple network status data.
- Case based reasoning based on simple network status data.
- Genetic algorithm based on simple network status data.
- Deep learning based on simple network status data.

7.3.1 Classification analysis of simple network status

Generally, simple network status data that is transformed from the basic network status data collected from the network can be classified into several known classes. Then, analysis can be performed based on the classified simple network status data and the causes that bring about those simple network statuses can be found.

For example, taking a single network device into account, if the simple network status information from the network device is 'connection lost', it can be classified into 'port link down', 'physical loss of signal' and 'software trouble of the peer' (another network device that connects with the network device through a physical or logical link), etc.

7.3.2 Cluster analysis for simple network status

The general process of cluster analysis method is similar to the process of classification analysis method. It needs also to divide the simple network status data into different categories. Then, the analysis can be taken based on those network categories.

Different from classification analysis method, network categories used in cluster analysis method are not pre-defined but extracted from the simple network status data.

For example, if the simple network status is 'event 1' and there are not any corresponding pre-defined categories, it can be classified into 'class 1' and the feature of ''class 1' comes from 'event 1' and similar network status data.

7.3.3 Correlation analysis of simple network status

The correlation analysis can be taken to shape the simple network status data while considering the following aspects:

- about correlated identical events: multiple identical events come from the same source;
- about correlated contrary events: multiple contrary events that are from the same source;
- about different events from the same source: multiple independent events come from the same source;
- about events from correlated event source: multiple events come from different sources that are related to each other.

7.3.4 Case based reasoning based on simple network status data

Regarding a certain kind of simple network status data, it is usual that a similar simple network status data can be found in the historical database that is used to store network status information. Under such a circumstance, a case based reasoning method can be applied.

There are following four steps to use case based reasoning for simple status data:

- Retrieve similar simple network status data in the corresponding database.
- Reuse the analysis result corresponding to the similar simple network status data.
- Revise the analysis result if required and if the revised result is better for the simple network status data.
- Retain the new similar simple network status in the corresponding database.

7.3.5 Genetic algorithm based on the simple network status data

A genetic algorithm aims to find the most appropriate individual from the entire population. It can be used to analysis simple network status data and find the most important event and true event source.

In the beginning, a group of two-tuple simple network statuses such as (O1, E1), (O1, E2)…(O1, En)…(Om, E1), (Om, E2)…(Om, En) can be achieved. Oi (i = 1, 2…*m*) represents the object where the corresponding event happens meanwhile Ej (j = 1, 2…*n*) represents different network events.

Then, a group of individuals can be achieved by choosing *m* two-tuple events (Oi, Ej) by a stochastic method. The group of individuals can be thought of as the entire population. The genetic algorithm can be applied to the population and the most appropriate individual can be thought of as the most possible event and event source.

7.3.6 Deep learning based on simple network status

Deep learning can also be used to analyse simple network status and find the most important event and true event source.

Take a group of two-tuple simple network status information (O1, E1), (O1, E2)…(O1, En)…(Om, E1), (Om, E2)…(Om, En) as the input, and build a deep neural network based on the aforementioned network status information, then the most important event Ei and the event source Oj can be found as output. O1, O2…Om represent the object where the corresponding event happens meanwhile E1, E2…Em represent different network events.

8 Mechanism of intelligent awareness for network fault

8.1 Overview of intelligent awareness for network fault

Intelligent awareness of network faults is responsible for sensing not only the network faults that have occurred but also the network faults that will possibly occur. In addition, intelligent awareness of network faults should attempt to trace the root errors of the network fault, predict the future network faults and give some suggestions to handle those network faults.

A complete process of intelligent awareness for network fault is illustrated in Figure 8-1. There are five main procedures as follows:

- Multiple-dimensional network status data collecting.
- Network fault correlation analysis based on multiple-dimensional data and machine learning.
- Root errors of the network fault tracing based on the aforementioned analysis and multiple-dimensional data.
- Future fault prediction based on the aforementioned analysis and multiple-dimensional data.
- Network fault related proposal generating based on machine learning.

It is noted that the process of intelligent awareness for network fault is repeated continuously and the result of the last process has impacts on the succeeding process.

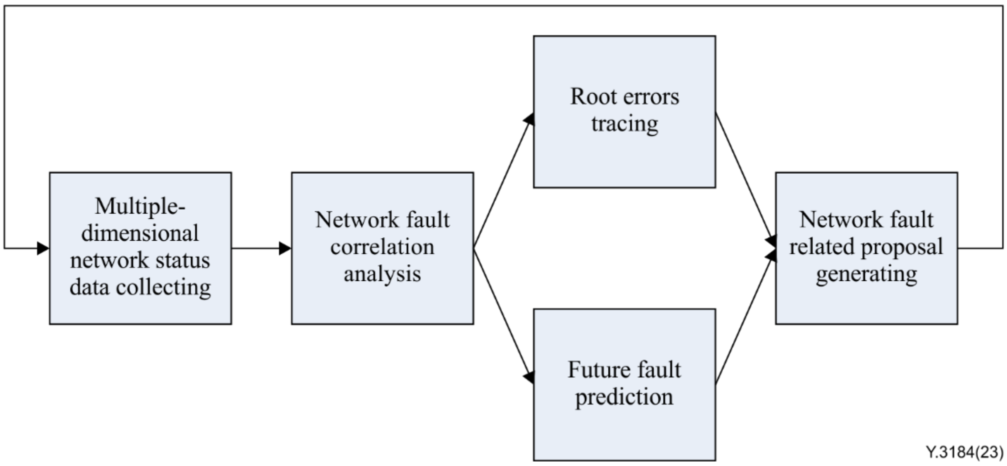

Figure 8-1 – Process for intelligent awareness for network fault

8.2 Multiple-dimensional network status data collecting

The process of intelligent awareness for network fault starts from collecting multiple-dimensional network status data. The aforementioned multiple-dimensional network status data refer to the following five aspects:

- Status data source object: the status data source is multiple-dimensional, in other words, the network status data are collected from various physical or logical objects such as network nodes, links or interfaces, environment, related databases and network management systems.
- Status data related objects: the status data is not only related to one class of objects, it also has a connection with multiple objects and multiple classes of objects.

  NOTE – The term 'objects' refers to entities, component or sub-components in the network, including physical and logical. For example, network device, port, connection are all objects.
- Status data representation: one kind of status data can have multiple representation formats such as binary, text, graph and audio.

• Status data classes: the classes of status data are also multiple-dimensional, that is to say that network resource status, network performance level, network service status, network environment, etc. should be taken into account.

• Status data impacts: the status data may have impacts on multiple network entities. Moreover, the status data may have impacts outside the network.

In a word, collecting multiple-dimensional network status data can be thought of as collecting all data that have possible impacts on network faults.

8.3 Network fault correlation analysis based on multiple-dimensional network status data

There are two main tasks that are required to be finished by the function of network fault correlation analysis based on multiple-dimensional network status data:

• Discover new possible network faults based on network status data and current network faults.

• Determine the relationship among different network faults and alarms.

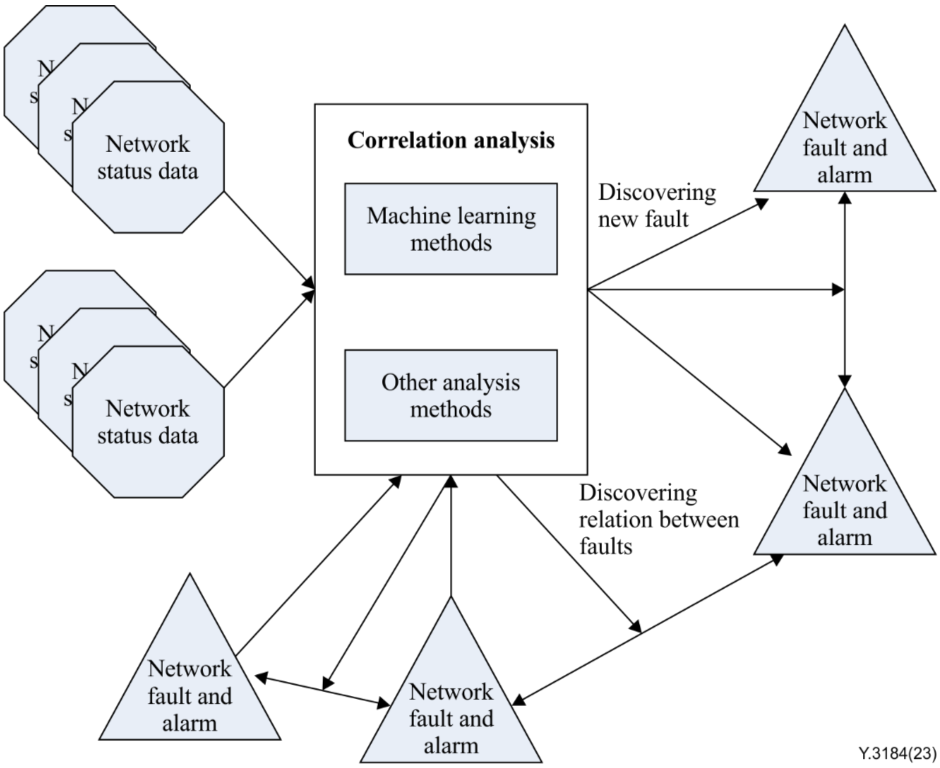

Figure 8-2 – Analysis for correlation of network faults

Figure 8-2 describes the process of analysis for network faults. All relevant network status data and present network faults and alarms are inputs of the correlation analysis function. Machine learning methods and other analysis methods can be used by the function. The analysis result is new network faults and the relationship between network faults and alarms.

8.4 Root errors finding based on the network fault tracing

It is recommended to find the root errors based on the analysis in clause 8.3 and multiple-dimensional status data if it is possible. Root errors are real reason for the network fault. It is therefore very important to trace the root errors of the network fault. When the root errors are fixed, the network fault will be also eliminated.

Figure 8-3 illustrates the procedure of root error tracing.

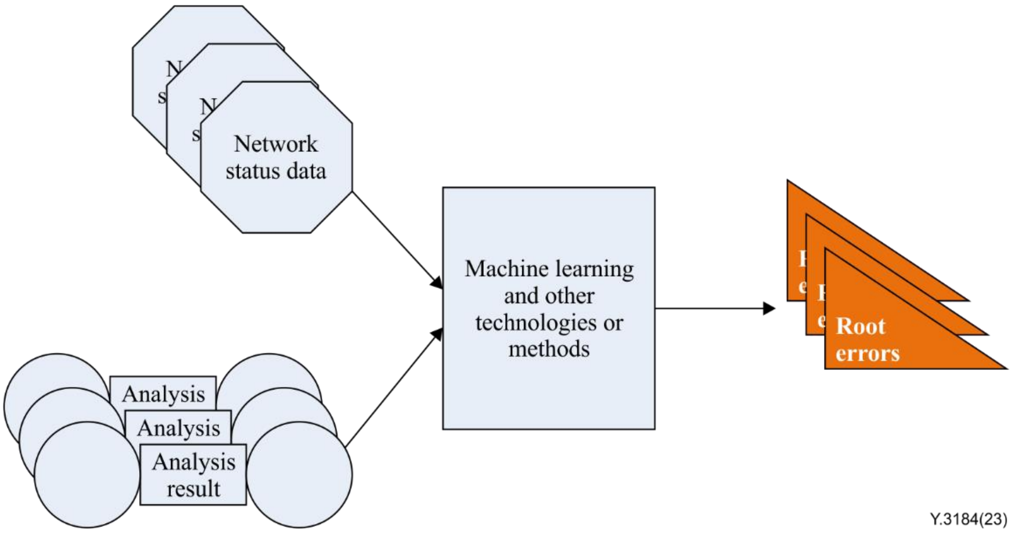

Figure 8-3 – Root errors of the network fault tracing

8.5 Future fault prediction

It is very useful and important to predict possible upcoming network faults, and this function is realized by the future prediction components. Figure 8-4 describes the process of future fault prediction. Machine learning methods are very appropriate for such a process, and with the help of such methods, possible upcoming network faults can be discovered based on network status data and current network faults and alarms.

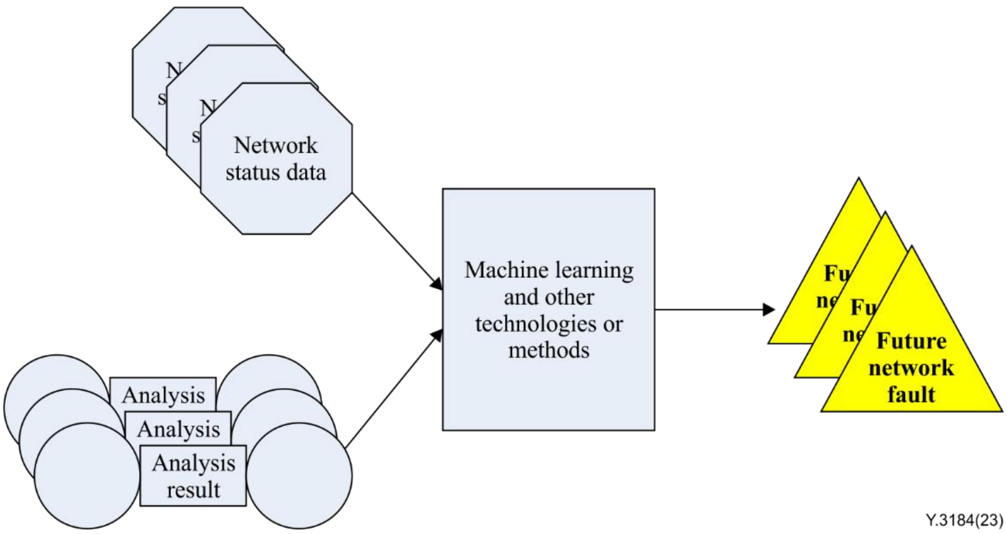

Figure 8-4 – Prediction for future possible network faults

8.6 Network fault related proposal generating

One of the targets for intelligent awareness of network faults is to improve network reliability and avoid future network faults. On the one hand, once the root errors have been found, it is required to report and give some proposals to elemented management system (EMS), network management system (NMS) and operation support system (OSS) in order that those systems and the corresponding operator can fix those root errors in time. On the other hand, after predicting potent network faults in the future, it is better to give some suggestions to avoid those network faults, and that is also the responsibility of proposal generating component.

Figure 8-5 illustrates how to generate action proposals. In Figure 8-5, machine learning methods are applied to find proper actions to avoid possible network faults.

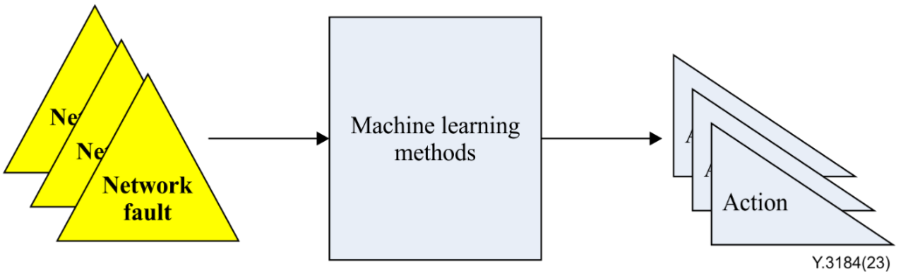

Figure 8-5 – Generating action proposal about future possible network faults

9 Mechanism for intelligent awareness of network performance

9.1 Overview of mechanism for intelligent awareness of network performance

The task for intelligent awareness of network performance is sensing the current performance situation, predicting future performance situation and bringing forward a proposal to improve the performance of the network.

Figure 9-1 depicts a complete process of intelligent awareness for network performance. There are four main procedures as follows:

- Network performance data collecting.
- Network performance data analysis.
- Future network performance predicting.
- Network performance proposal generating.

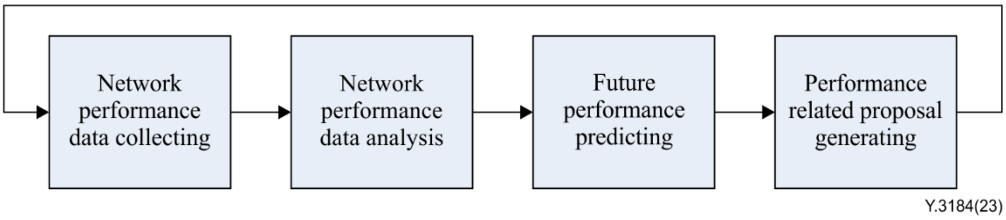

Figure 9-1 – Process for intelligent awareness for network performance

It is noted that the process of intelligent awareness for network performance is also a cycled process and the result of the last process possibly has impacts on the succeeding process.

9.2 Directly performance data collecting

The first procedure of the process for intelligent awareness of network performance is collecting various performance data from the network. The raw performance data are generated by the network node directly. The following are some classes of raw performance data:

- Latency related performance data.
- Latency variation related performance data.
- Traffic throughout related performance.

9.3 Analysis for the collected performance data

The second procedure of the process for intelligent awareness of network performance is analysing the collected performance data. There are two main aspects for the analysis as follows:

- Performance analysis.
- Performance and resource correlation analysis.

9.3.1 Performance analysis based on machine learning

After the raw performance data have been collected, the succeeding step of the process for intelligent awareness of network performance is analysing the raw performance data based on machine learning.

There are two classes of the above analysis as follows:

- Time related performance: Analysing the law between the time and the raw performance.
- Space related performance: Analysing the law between the network physical partition and the raw performance.

9.3.2 Performance and resource correlation analysis based on machine learning

The next operation of the process for intelligent awareness of network performance is analysing the relationship between the performance data, the network resource configuration and the network traffic based on machine learning.

There are also two classes of the above analysis as follows:

- Correlation analysis for performance data and network resource configuration: keeping network traffic unchanged, analysing the law between performance data and network resource configuration.
- Correlation analysis for performance data and network traffic: keeping network resource configuration unchanged, analysing the relationship between performance data and network traffic.

9.4 Performance prediction based on machine learning

The third step of the process for intelligent awareness of network performance is predicting the future performance status in advance. In other words, through the historical performance data and machine learning, the future performance can be predicted.

Combining the result of performance related analysis described in clauses 9.3.1 and 9.3.2, a relation model between performance and factors that have impacts on network performance can be acquired. The aforementioned factors include time, space, network resource and network traffic.

Then, as a certain upcoming epoch, those factors can be estimated, and the performance situation related to the epoch can be predicted based on the relation model.

9.5 Performance related proposal generating based on machine learning

The last step of the process for intelligent awareness of network performance is generating some useful suggestions for network operators or network service providers. Those suggestions can be reported to EMS, NMS or OSS/BSS, etc.

For example, if during a certain future period, a certain network partition is possibly congested based on network performance intelligent awareness, the proposal should be brought forward to the network operator or network service provider in order that the network operator or network service provider can deploy or schedule more network resources in order to avoid congestion.

10 Mechanism for intelligent awareness of network resource

10.1 Overview of mechanism for intelligent awareness of network resource

Another important network status is utility of network resource. Network resource directly decides performance of the network, and network fault possibly occurs if network resource cannot meet the requirements of necessary network service. So, it is also very important to grasp the situation of network resource accurately, and it is the task for intelligent awareness of network resource.

A complete process for intelligent awareness of network resource mainly contains the following four stages:

- Network resource data collecting.
- Network resource utility analysing and modelling.
- Network resource utility predicting and lifetime managing.
- Network resource related proposal generating.

The following aspects for intelligent awareness of network resource are recommended to be taken into account. It is noted that the function of intelligent awareness of network resource is not limited to those aspects:

- Intelligent awareness to utility of network bandwidth resource.
- Intelligent awareness of utility of network computing resource.
- Intelligent awareness of utility of network queue resource.
- Intelligent awareness of utility of network storage resource.

Figure 10-1 describes the process of intelligent awareness of network resource.

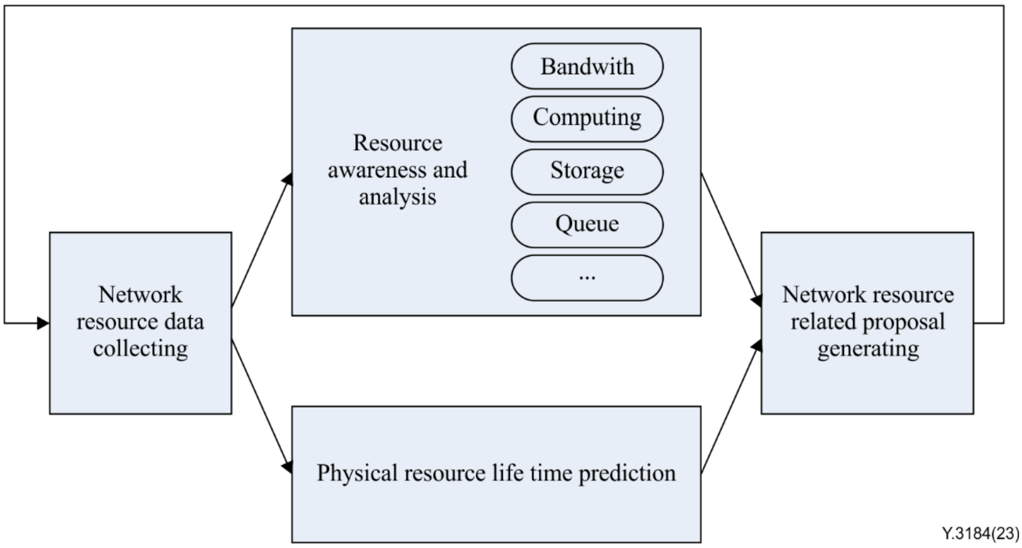

Figure 10-1 – General process for intelligent awareness for network resource

10.2 Network resource data collecting

This is also the first step of the process for intelligent awareness of network resource to collect network resource data.

Some network resource data can be collected from the network directly, for example, network designed bandwidth information can be obtained from the port feature of a network device. Some other resource data need to be obtained through computing, for example, CPU utility data cannot be acquired directly and some computation is necessary.

Collected network resource data is used for analysing and modelling.

10.3 Network resource awareness and analysis

The mechanisms for network resource data analysing and modelling possibly differ with different network resources. That is to say, network bandwidth data analysing and modelling is possibly different from network computing resource data analysing and modelling. In order to illustrate the mechanism more clearly, the mechanism of data analysing and modelling for the following network resource will be illustrated independently:

- network bandwidth resource.
- network computing resource.
- network queue resource.
- network storage resource.

10.3.1 Intelligent awareness mechanism for resource utility of network bandwidth

Network bandwidth is one of the most important resources of the network. Generally, the data transport volume strongly relies on the network bandwidth. So, an awareness of network bandwidth resources is very beneficial to planning and scheduling the network traffic that is carried on the network.

It is possible to know the designed network bandwidth of the network and be aware of the currently available network bandwidth in real-time. Although current bandwidth information is still important for network control and management, it is not enough to provide good network service, schedule network resources efficiently and optimize the network reasonably based on current bandwidth information. For example, if the target that the high network bandwidth utility should be achieved means network congestion should be avoided, the future bandwidth utility should be aware in order that network resource reschedule, network route re-computing and network re-structure can be carried out in advance in order that the scheduled network bandwidth accurately matches the network traffic.

So, the following mechanism of intelligent awareness of network bandwidth is recommended to be used so that network bandwidth can support the network service while no waste of network bandwidth occurs.

Let 'L' represent a certain network link, 'Bd' represent a designed network width of L, 't' represent time, 'St' represent the network traffic of L at time t, 'Bt' represent available bandwidth at time t and 'Ut' represent network bandwidth utility at time t. The following two equations (10-1 and 10-2) apply:

$$Bt = f\,(Bd, St, t) \tag{10-1}$$

$$Ut = (1 - Bt/Bd) \times 100\% \tag{10-2}$$

Then, the task of intelligent awareness of network bandwidth utilization can be changed to finding the function 'f'. In order to find the most optimal value of f, machine learning methods together with the other method can be used. For example, deep learning methods can be used to find the most optimal value of f based on the aforementioned variables such as 'Bt'.

When 'f' is achieved, 'Bt' and 'Ut' can be computed and network traffic and network bandwidth can be rescheduled in advance in order to achieve high network bandwidth utility without congestion.

The intelligent awareness process of network bandwidth resource utilization includes directly collecting the bandwidth utilization of each link in the network, analysing the changing trend of link bandwidth, predicting link bandwidth bottleneck, adjusting bandwidth allocation according to network bandwidth utilization and avoiding the formation of network congestion.

The raw bandwidth data is generated directly by the network nodes. The following are some classes of raw bandwidth data:

- Bandwidth utilization of each port.
- Bandwidth utilization of each link.
- The packet transmission rate of each link.
- The bit transmission rate of each link.

NOTE 1 – In this Recommendation, a port is the physical port of a device in network, such as the Ethernet port of a router in a network.

NOTE 2 – In this Recommendation, a link is a physical junction or multiple physical junction aggregation of a network node to its adjacent node in a network. For example, a physical connection line between two adjacent routers in a network.

10.3.2 Intelligent awareness mechanism for resource utility of network computing

Network computing resource is also an important resource of the network. It should be noted that the aforementioned network computing resource is not a generalized computing resource for computing and network convergence but a special computing resource used for network schedule, control and management.

Similar to network bandwidth resources, it is helpful to be aware of future computing resource utility. Then, some measures can be taken to ensure good network computing resource utility.

The following mechanism of intelligent awareness of network computing resources is recommended to be used in order to prevent computing resource overload or waste of the computing resources.

Let '*D*' represent a certain network device, '*t*' represent time, '*Tt*' represent the network traffic to be processed by network computing resource at time *t*, '*Ut*' represent real network computing utility at time *t* and '*Utp*' represent real network computing utility at time *t*. The main task for the intelligent awareness of network computing resources is to find an approach to make '*Utp*' almost equal '*Ut*'. The task of intelligent awareness of network computing resource utility can also be changed to finding the computing methods to obtain a '*Utp*' value based on '*Tt*' and '*t*', etc. Similar to the situation described in clause 10.1, machine learning methods can be used to find computing methods.

The intelligent awareness process of network computing utilization includes directly collecting the computing power and utilization of each node in the network, analysing the changing trend of the CPU utilization and the main reasons for the CPU utilization change, predicting the computing power bottleneck in the network, and generating the processing method that the CPU utilization is lower than the threshold.

The raw CPU computing power and utilization data are generated directly by the network nodes. The following are some classes of raw data:

- CPU processing power of each network node.
- CPU utilization of each network node.
- The computing resource utility proportion of various services in a network node.

10.3.3 Intelligent awareness mechanism for utility of network queue resource

The intelligent awareness process of network queue resource utilization includes directly collecting the queue resources and utilization of each node in the network, analysing the changing trend of queue resource utilization of each network node and the main services affecting the queue resources, predicting the queue resource capacity bottleneck of network nodes and generating the service forwarding rule of efficient queue resource utilization.

The awareness process of network queue resource utilization first collects the queue quantity and the utilization of each queue from the network node. The raw network node queue resource utilization is generated directly by the network nodes. The following are some classes of raw data:

- The queue quantity of each network node.
- Each queue length of each network node.
- The queue scheduling algorithm and corresponding threshold parameter.
- The queue utilization of each network node.
- The distribution of services to be forwarded in each queue of the network node.
- The distribution of packets to be forwarded in each queue of the network node.

NOTE – The queue resource utility reflects the traffic burst of the network node. If the queue utilization changes dramatically, it means that the node has a traffic burst or micro-burst, jitter performance deteriorated, congestion may have happened in the network, and so on. Thus, the queue resource utility is critical to network quality and needs to be aware.

10.3.4 Intelligent awareness mechanism for resource utility of network storage

Network storage resource is also necessary for the network. Similarly, the aforementioned network storage resource is not a generalized storage resource for computing and network convergence but a special storage resource used for network data forwarding, control and management.

It is also beneficial to be aware of the future storage resource utility. Then, some actions can be taken to make the network storage resource utility secure.

The following mechanism of intelligent awareness of network storage resources is recommended.

Let '*D*' represent a certain network device, '*t*' represent time, '*Tt*' represent the network traffic to be stored in the network storage resource at time *t*, '*Ust*' represent real network storage utility at time *t* and '*Ustp*' represent real network storage utility at time *t*. Then the target for the intelligent awareness of network storage resource is to find an approach to make '*Ustp*' almost equal to '*Ust*'. So, the task of intelligent awareness of network storage resource utility can also be changed to finding the computing methods to get a '*Ustp*' value based on '*Tt*' and '*t*', etc. As in clause 10.1, machine learning methods can be used to find the computing methods.

The intelligent awareness process of network storage resource utilization includes directly collecting the storage resources and utilization of each node in the network, analysing the changing trend of storage resource utilization of each network node, predicting the bottleneck of storage resource capacity of network nodes, and generating the processing method that the storage resource utilization of network nodes is lower than the threshold.

The awareness process of network storage resource utilization first collects the storage quantity and utilization from the network node. The raw network node storage resource utilization is generated directly by the network nodes. The following are classes of raw data:

- The queue number of each network node.
- Storage sizes of the network nodes.
- Storage utilization of network nodes.
- Storage files and sizes of network nodes.

10.4 Physical resource lifetime prediction

All physical resources have a limited lifetime, and the probability that a certain physical resource is out of order will rise when the physical resource is near the end of its lifetime. It is therefore very beneficial to predict the lifetime of the physical resource because it helps to monitor and upgrade the physical resource in time.

The following mechanism can be used to predict the lifetime of the physical resource.

Let '*D*' represent a certain physical resource such as a network device, '*t*' represent current time, '*ts*' represent the time the physical resource begins to work, '*tw*' represent the accumulative time the physical resource is powered on, '*F*' represent the temperature, '*H*' represent humidity, '*O*' represent other environment indexes, '*L*' represent the normal lifetime of the physical resource and '*Ll*' represent the left lifetime of the physical resource. Then the task for predicting the lifetime of the physical resource is to find an approach to obtain the value of '*Ll*' based on '*L*', '*t*', '*ts*', '*tw*', '*F*', '*H*' and '*O*'. As in clause 10.1, machine learning methods can be used to find the aforementioned approach.

After collecting the raw network resource utilization data, the second step of network status intelligent awareness is to analyse the raw resource utilization data based on machine learning, similar to the second step of fault awareness and performance awareness described in the previous clause. The third step is to analyse resource utilization correlation, including the following correlation:

- The cycle of the network resource utilization variation.
- The relationship between network resource utilization and network performance.
- The relationship between network resource utilization and fault.

10.5 Physical resource proposal generating based on machine learning

The fourth step of network status intelligence awareness is to generate adjustment suggestions for physical resources according to collection, analysis and prediction, so as to avoid resource bottlenecks and congestion in the network.

A machine learning method is adopted to find the suitable adjustment mechanisms, such as the change of some service forwarding paths, the modification of network node parameters and so on. This is to realize the efficient utilization of network physical resources.

When the process for intelligent awareness of the network resource is completed, some network status information about the network resource can be acquired and this network status information can be used to control, manage, plan and optimize the network.

Some important aspects of network status information are about the physical resource utility and lifetime of the physical resource. Those information aspects can be used to generate some proposals to the network owner or the network operator.

When the physical resource utility is reaching a certain threshold, a proposal that network traffic should be re-scheduled or more physical resources should be deployed in the network will be brought forward.

11 Mechanism for intelligent awareness of network load

11.1 Overview of mechanism for intelligent awareness of network load

Network load refers to the network traffic carried on the network. The task for intelligent awareness of network load is sensing current network traffic status, evaluating the situation as to whether the network resource can support the network traffic, predicting future network load and bringing forward a proposal to improve the situation for the network to meet the requirements of the network load.

Figure 11-1 depicts a complete process of intelligent awareness for network load. There are four main procedures as follows:

- Network load data collecting.
- Correlation analysis for network load&resource&time.
- Future network load predicting.
- Related proposal generating.

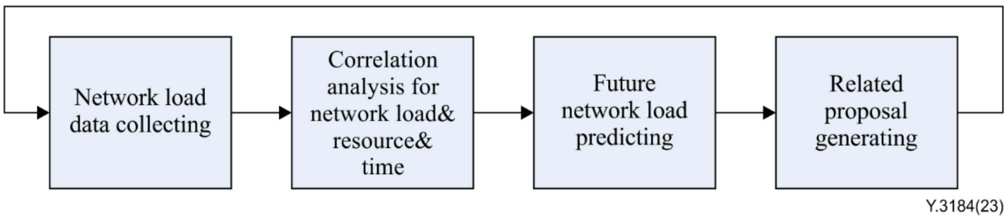

Figure 11-1 – Process for intelligent awareness for network load

It is noted that the process of intelligent awareness for network load is also a repeated process and the result of the last process possibly has impacts on the succeeding process.

11.2 Network load data collecting

The first procedure of the process for intelligent awareness of network load is collecting various network load data from the network. The following are classes of raw network load data:

- Network load corresponding to an application/service.
- Network load corresponding to a physical port.
- Network load corresponding to a network node.
- Network load corresponding to a network route.
- Network load corresponding to a network domain.

Some representative methods such as DPI (see [ITU-T Y.2770] and [ITU-T Y.2771]) and deep flow inspection (DFI, a packet filtering technique that analyses statistical characteristics such as packet lengths, ratio of large packets and small payload standard deviation, and connection behaviour of flows) can be used to collect network load data.

11.3 Correlation analysis for network load&resource&time

The second procedure of the process for intelligent awareness of network load is analysing the collected network data. There are three main aspects for the analysis as follows:

- Correlation analysis for network load and time.
- Correlation analysis for network load and resource.
- Correlation analysis for network load, time and resource.

One of the tasks for correlation analysis for network load, time and resource is evaluating the situation as to how the network resource can support the network load. An evaluation index named traffic overload rate 'O' can be used to describe the aforementioned situation. Let 'Tr' represent the real-time network load and 'Td' represent the maximum network load that the network can support without any data loss, then 'O' can be calculated by equation (11-1):

$$O = Tr / Td \qquad (11\text{-}1)$$

Let 't' represent time, 'R' represent the quantitative network resource. Then the relationship among 'O', 't', 'Tr' and 'R' can be described as:

$$O = F(t, R, Tr) \qquad (11\text{-}2)$$

'F' representative the function that describes the aforementioned relationship and it can be achieved by correlation analysis of the four indexes. If 'F' is confirmed, the evaluation index 'O' can be obtained and this reflects how the network resource can support the network load. If 'O' is less than or equal to 100%, the network resource can support the network load. On the contrary, If 'O' is greater than 100%, the network resource cannot support the network load.

11.4 Future network load prediction based on machine learning

The third step of the process for intelligent awareness of network load is predicting the future network load in advance. In other words, through the history network data and machine learning, the future network load can be predicted.

The main task of future network load prediction is finding a relationship between network load and time. The relationship can be described as follows:

$$Tr = g\ (t) \qquad (11\text{-}3)$$

The function '*g*' represents the relationship between time *t* and network load *Tr*. When the function '*g*' is confirmed, the value of *Tr* in a future epoch *t* can be predicted.

11.5 Network load related proposal generating based on machine learning

The last step of the process for the intelligent awareness of network load is generating some useful suggestions for network operators or network service providers.

For example, if during a certain future period, overload will possibly happen on a certain network route based on intelligent awareness of the network load, the proposal should be brought forward to the network operator or network service provider in order that the network operator or network service provider can re-orchestrate and reschedule the network load on different routes and avoid overload.

12 Mechanism for intelligent awareness of other network statuses

12.1 Mechanism for intelligent awareness of network physical environment

The network physical environment includes network node availability, network connection availability, network environment, etc. Awareness of the network physical environment can be classified into two types.

NOTE – A network node refers to a network device deployed in the network, while network connection means a connection between two network nodes.

Network environment awareness: The information used by environment awareness function includes environmental information such as the operating temperature and humidity of network nodes. The environmental information of generic network nodes can be perceived by sensors. For example, mobile node environmental information can be obtained by using RF sensing, cellular networks sensors and other resource sensing methods based on wireless communication technology.

Network physical status awareness: The information used by the network physical status awareness function includes network node location, active status of network node, operational status of network devices, topology changes of network connections, etc. A function called network status sensing can be used to obtain network status information.

In reality, network performance deeply depends on the network physical environment. For example, if the temperature of the physical environment changes, the performance of the network device will also change.

Although it is important for the network control system or NMS to know the parameters of the physical environment such as temperature, moisture and pressure and so on, the key factor of intelligent awareness of the network physical environment is not aware of the value of environment parameter.

It is more important to find the relationship between network performance and network environment parameters, then network control and management can be implemented on the basis of the aforementioned relationship. The aforementioned law can be described by equation (12-1):

$$P = G\ (F1, F2...... Fn) \qquad (12\text{-}1)$$

Equation prepresents network performance and can also be a vector including a group of parameters such as throughput, latency, jitter and so on. *F*1, *F*2....... and *Fn* each represents a kind of environment parameter. *G* represents a function that depicts the relationship between *P* and *F*1, *F*2......and *Fn*.

Equation (12-1) can only describe the relationship between network performance and environment parameter. However, network performance is also a function about itself; in other words, current network performance can also influence the future network performance, so the following formula can describe the relationship between network performance and environment parameter accurately.

$$P(tj) = H(F1, F2...... Fn, P(ti)) \qquad (12\text{-}2)$$

H represents the updated function, *P*(*ti*) and *P*(*tj*) represent the network performance at epoch *ti* and *tj* respectively; *tj* is later than *ti*.

The aforementioned functions *G* and *H* can be built on the basis of the historical data. Taken it as a simple example, the following table can be used for describing *H*.

Table 12-1 – Example of function *H*

Network performance environment index	**Throughput (*tj*)**	**Latency (*tj*)**	**Jitter (*tj*)**	**...**	**Computing performance**
Temperature					
Moisture					
Pressure					
....					
Throughput (*ti*)	*P*1(*tj*)	*P*2(*tj*)	*P*3(*tj*)		*Pn*(*tj*)
Latency (*ti*)					
......					

Intelligent awareness of the network physical environment includes also four steps: data collection, data analysis, state assessment and situational prediction. These are shown in Figure 12-1.

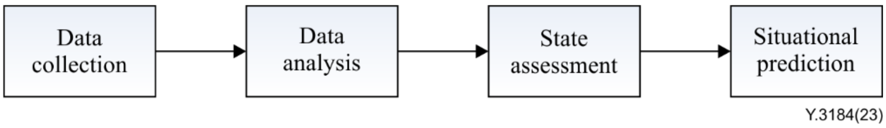

Figure 12-1 – procedure for network environment awareness

Data collection: Through a variety of detection methods, data related to a group of factors that affect the status of the network and devices in the network are detected and collected.

Data analysis: All kinds of status data of network and network node are processed by means of classification, merging and transformation at first. Then this processed information is analysed comprehensively to derive the overall influence factor related to the network.

State assessment: Qualitative and quantitative analysis of result of data analysis, following which, the corresponding countermeasures are given.

Situational prediction: The data output from the state assessment is used to predict the network status changes and topology changes of the network in the future.

12.2 Mechanism for intelligent awareness of network partner context

The network function, performance and service of a network not only depend on the network itself but also influence or are influenced by the other networks. If network B can influence the network function, performance and service of network A or network function, the performance and service of network B are possibly influenced by network A, and then network A and network B are network partners.

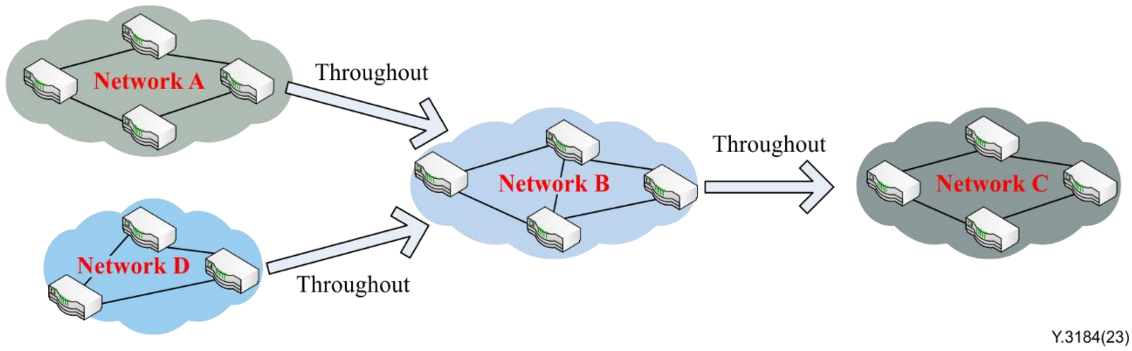

Figure 12-2 – Relation between network partners

Figure 12-2 shows a simple description of network partners, where network A, C and D are all network partners of network B. Influence between a pair of network partners is possibly unidirectional or bidirectional. For example, Network A and network B are a pair of network partners and it is certain that network A has a direct influence to network B. However, when there is a flow-control mechanism between network A and network B, network B can also influence network A indirectly.

Because the network partner of a network can influence the network performance of the network directly or indirectly, it is beneficial for the network to be aware of the context of its network partners. Although it is much more difficult to be aware of the context of a network partner, there are still three feasible methods to implement intelligent awareness of the network partner context:

- Rely on the network partner itself.
- Rely on the centralized controller.
- Through network traffic analysis.

Relying on the network partner itself: If there are some interfaces or paths for network partners to exchange information directly, the information of the network context can be shared with network partners through the interfaces or paths.

Relying on centralized controller: If there is not an interface or path for network partners to exchange information directly and there are one or more centralized controllers that can control both the network partners, the information of the network context can be shared with its network partners through the centralized controllers. Figure 12-3 shows such a scenario.

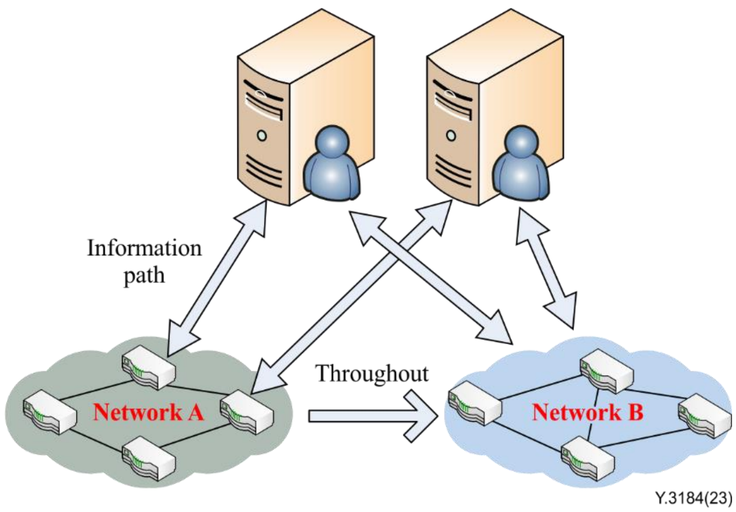

Figure 12-3 – Context information shared through controllers

Through network traffic analysis: If there is not an interface or path for network partners to exchange information directly and there is not a centralized controller that can control both the network partners, the information of the network partner context cannot be shared with the network. Then, the network can only obtain the information by itself and it can be implemented through network traffic analysis.

Figure 12-4 shows a network partner context model for intelligent awareness. It consists of three main layers:

- network status sensing layer
- context aware layer (the same as network status analysis layer in Figure 7-1)
- application layer (the same as network status reporting and display in Figure 7-1).

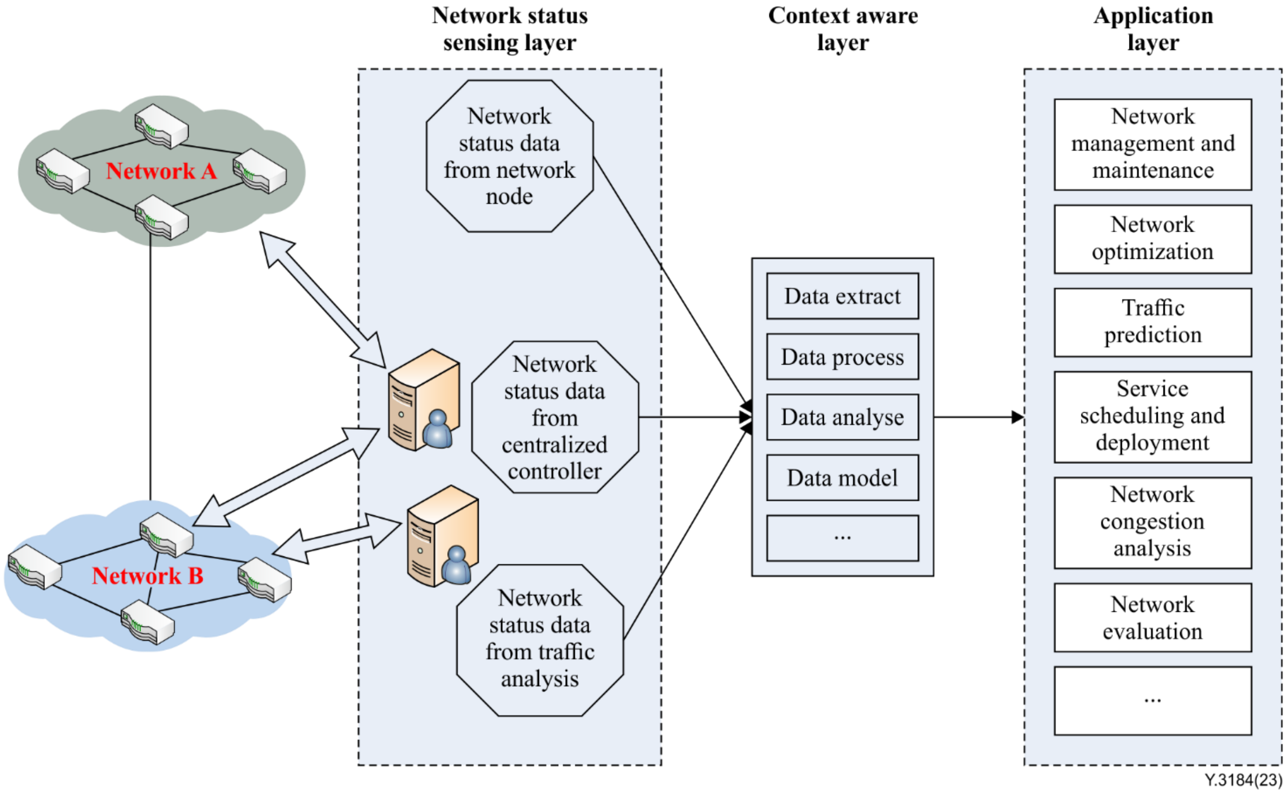

Figure 12-4 – Intelligent awareness of network partner context model

Network status sensing layer: The network status sensing layer mainly includes various sensing network nodes. For example, it relies on the network partner itself or the centralized controller. The sensing network node collects various types of contextual information from various types of resources containing contextual information (physical or virtual resources) and uploads them to the context aware layer.

Context aware layer: The context aware layer uses context information, such as context type and value information, timestamps and context attributes. The context aware layer filters, merges and normalizes the collected data. This processing includes context modelling, context extracting, context information merging, context information distribution and context detection, etc. Through a series of processing of the low-level context information, the high-level context information is obtained.

Application layer: The application layer applies the high-level contextual information obtained from the context aware layer processing to the information service application. The application layer enables automatic interaction with the user and provides the required functionality. Such as data distribution, routeing selection, energy monitoring, location services, content adaptation delivery, recommendation services, etc.

13 Security consideration

The mechanisms specified in [ITU-T Y.2704] address the security requirements of this Recommendation. In addition, entities and the information pertaining to the mechanism specified in this Recommendation should be under protection against threats described in [ITU-T Y.2704] and [ITU-T F.747.10].

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

Published in Switzerland
Geneva, 2023