Conscious Network That Enables Autonomous Operation and Maintenance

● Takuya Nitta ● Yasuhiko Aoki ● Kyoko Ohya ● Fumiyuki Iizuka
● Toshiki Honda

Today, networks connect computing resources, front devices, and applications that are scattered across many places, including those on-premise and in the cloud, allowing people and society as a whole to enjoy diverse services. However, a failure or degradation of a network has the potential to cause considerable problems to connected devices and services. To prevent these risks, a "conscious" network system with autonomous operation and maintenance capabilities will be required. Such a system will detect the slightest irregularities in the network as early signs of errors and prevent possible failures or degradation from occurring. It will also ensure that the services remain available without having to modify end users' systems or make users aware of the network problems. To realize such systems, Fujitsu has been working on development of the technologies necessary for integrated network monitoring: detection of early signs through Internet Protocol (IP) packet behavior analysis and optical transport signal quality monitoring, optical wavelength reassignment, and self-diagnosis for IP networks. This paper describes these technologies required for the realization of the conscious network.

1. Introduction

In recent years, due to the decrease in maintenance and operation man-hours required for ICT infrastructure and networks, enhanced security, and increasing demand for teleworking, cloud services have come to be equipped with functions conventionally provided by devices and on-premise servers. Services may be offered across multiple clouds. Furthermore, services have come to be provided across virtual and business-oriented networks, in addition to the wavelength-division multiplexing (WDM), Internet Protocol (IP), and wireless networks on which they are placed.

Accordingly, when service response is delayed or any service becomes unavailable, it is necessary to isolate the problem in order to identify the cause—the application or the network. If the problem is in the network, however, it is difficult to identify the location in the network where the quality degradation or failure has occurred. As a result, problems are increasingly showing a tendency to take a long time to solve, and how to deal with this poses an issue.

Recently, because the IoT has caused the volume of data and use of cloud services to increase, fixed broadband access and mobile communications services have expanded, and infrastructure in the form of optical networks to support them are increasingly in use. These optical networks use ultra-high capacity optical fiber networks of 100 to 400 Gbps and, should a problem occur, an enormous number of services, users, and IoT devices may be affected. In order not to stop optical networks, which have become a social infrastructure, the capability to detect early signs of failures and deal with these failures by diverting communications to new paths or by increasing the communication bandwidth is required.

To quickly identify the failure points as described above and operate services with safety and security, Fujitsu attaches importance to integrated monitoring and operations across communication layers (physical, virtual, and business-oriented) from end to end by detecting early signs of failures.

This paper first proposes the operation and monitoring technology for autonomously preventing failures by detecting early signs of failures with the concept of conscious networks. It then describes the technology for early sign detection required to prevent network

failures and the technology for maintaining service quality.

2. Conventional technologies and issues with them

Conventionally, network monitoring was achieved by poll monitoring using a combination of Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP) or using either SNMP or ICMP and messages output from devices such as trap and syslog messages to detect failures in devices. The failures were then handled as needed. For this reason, problems could be dealt with only after they occurred, even if service continuity was maintained through network path diversion, and impacts on services were unavoidable.

In addition, silent failures,[note)] in which failures are caused by internal failures of network devices but the devices themselves are unable to detect the failures, could not be dealt with in the first place.

Furthermore, network monitoring systems were set up individually for WDM networks, IP networks (including core networks, access networks, and data center internal networks) and wireless networks, and monitored and operated independently. This not only led to low operational efficiency but also to a large amount of time required to identify the failure points, resulting in a long time taken before services could be restored.

3. Conscious networks

In order to solve the problems mentioned in the previous section, Fujitsu studied network enhancement. Consequently, we have proposed a concept called conscious network, which maintains end-to-end service quality by making use of our network-related analysis and visualization technologies to detect early signs of failures before they occur and providing autonomous control.

To realize this concept, we are developing technologies to expand scenarios, including early sign detection, failure isolation, cause identification, resource optimization, and path diversion on a platform where data from multi-layer network such as IP networks and optical transmission and multi-vendor devices are collected, integrated, and analyzed.

The following sections describe technologies for realizing the conscious network: IP packet behavior analysis technology and early sign detection technology through optical transmission device signal quality monitoring analysis, which are needed to prevent network failures; optical signal accommodation optimization technology for maintaining service quality; and self-diagnosis technology for IP networks.

4. Technologies for preventing network failures

4.1 IP packet behavior analysis

If degradation of network devices or cables or intermittent failures due to network device firmware bugs cannot be detected by the devices themselves, they present themselves as events such as packet losses and roundtrip time (RTT) degradation.

FUJITSU Network Proactnes II QM, which supports network maintenance and optimization, captures packets that flow in a network and makes use of the characteristics of the Transmission Control Protocol (TCP) to analyze them. In this way, it measures the end-to-end communication quality in terms of packet loss, RTT, and so on. Detection of early signs of failures and silent failures is achieved by detecting these packet losses and instances of RTT degradation. In addition, measurement of end-to-end communication quality allows the communication quality to be grasped for individual sources and destinations. Accordingly, points causing degradation of communication quality can be narrowed down simply by setting up the QM at a point where traffic is concentrated and capturing packets (**Figure 1**).

For detection of failure points, TCP sequence analysis is first used to isolate suspected points based on the quality of four sections centered around the capture point: transmission and reception between the client and the capture point, and transmission and reception between the capture point and the server. Then, the trend in degradation is analyzed based on the end-to-end communication quality information and key information such as the network addresses and virtual LAN Identifiers (VLAN-IDs) according to the

note) Failures that cannot be detected by network devices themselves using the autonomous diagnosis function.

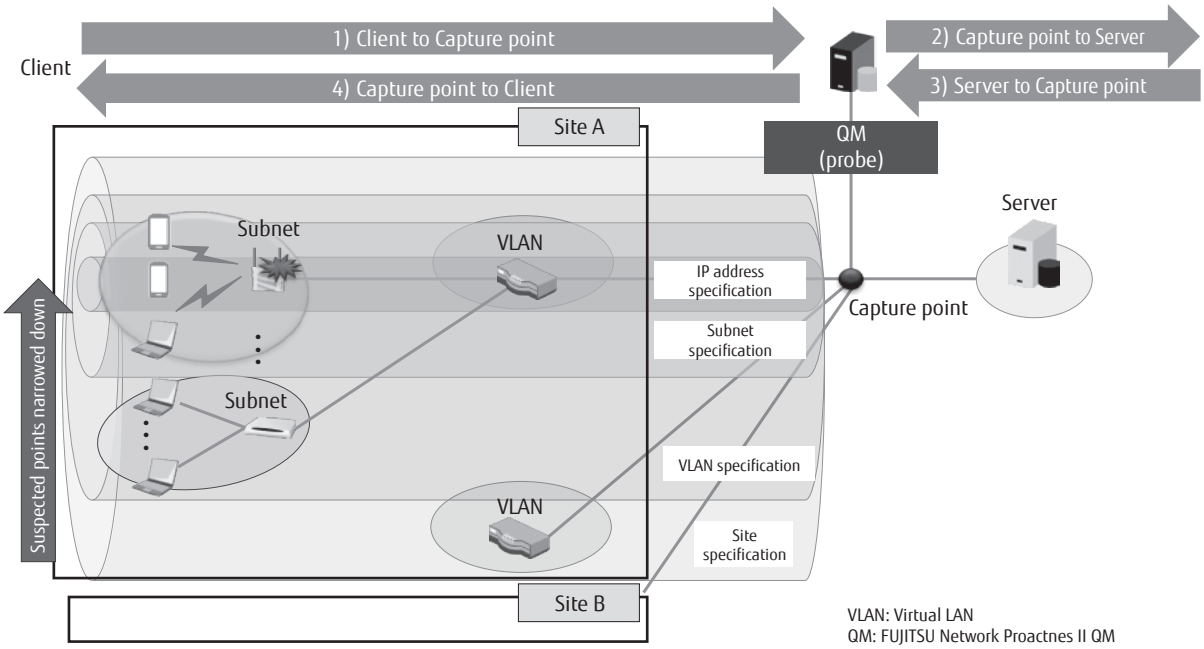


Figure 1
End-to-end Isolation of failure points.

target network configuration. This narrows down the suspected points.

Methods for narrowing these down include identifying points using IP addresses and routing information and identifying points based on V-LAN IDs. In an overlay network that applies Virtual eXtensible LAN (VXLAN), Ethernet frames are encapsulated in User Datagram Protocol (UDP)/IP and inner TCP sessions (part of Ethernet frames before encapsulation) are used to evaluate the communication quality. The results can be aggregated based on inner IP addresses to identify logical degradation points, and based on outer IP addresses (UDP/IP for encapsulation) to identify physical degradation points.

In this way, analysis of end-to-end communication quality allows devices and cables with problems to be identified quickly. At the same time, detailed analysis such as degradation analysis of optical transmission paths as described below can be performed quickly.

4.2 Optical transmission device signal quality monitoring analysis

With WDM transmission, a system with a transmission speed of 600 Gbps per wavelength and a transmission capacity of 76.8 Tbps[1)] per fiber is nearing practical application. The operation of optical networks, which was conventionally handled primarily by communications carriers, is expanding to include enterprise users as in data center interconnect (DCI) connecting large-scale data centers.

In this way, WDM transmission systems are positioned as a platform to support various tasks across locations on premise and in the cloud. WDM transmission systems are increasingly gaining importance. Given this situation, expectations regarding the avoidance of large-scale failures are increasing via the detection of early signs of system failures through the visualization and analysis of optical network operations.

Figure 2 shows early sign detection of failures in an optical network. The optical transmission nodes are equipped with a performance monitor (PM) function to monitor signal quality such as the intensity of optical signals, and these functions are used as sensor devices in the optical network. PM information, which was conventionally used only for monitoring the status of devices before and after failures and alarms, is continuously stored as log data and analyzed with machine learning. This is used to detect early signs of failures in the optical transmission system and identify failure

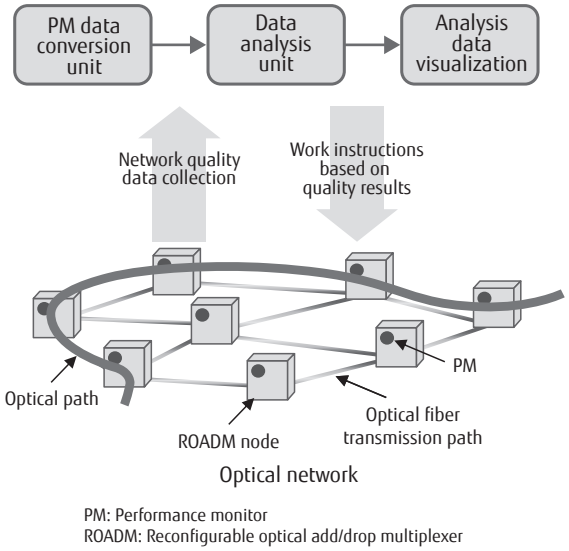


Figure 2
Detection of early signs of failures in optical network.

points.

The input and output of optical transmission devices, design values of optical signals, and degradation of optical signals in the optical transmission system are grasped with machine learning and the points of degradation and their causes are analyzed. In this case, the connections between the reconfigurable optical add/drop multiplexer (ROADM) nodes and optical fiber transmission paths as well as the information about the optical paths (start points, end points, and intermediate nodes) are used.

5. Technologies for maintaining service quality

5.1 Optical wavelength assignment optimization

Concerning optical networks, expectations are increasing for increased utilization efficiency of wavelength resources in order to efficiently accommodate ever-increasing traffic. Meanwhile, the number of optical wavelength (optical signal bandwidth) that can be accommodated in optical fiber is restricted by the system configuration. In addition, to connect optical signals without going through a regenerative repeater, there was a need to accommodate signals without wavelength conversion. However, the increase in accommodating services causes a phenomenon in which wavelength fragmentation occurs, hindering utilization of wavelength resources. In particular, this phenomenon is conspicuous in optical networks with a mesh topology composed of ROADM nodes as shown in **Figure 3 (a)**.

To solve this problem, we have developed an optical wavelength reassignment technology (algorithm) that relocates fragmented optical wavelength resources in a manner that does not affect the service to regenerate usable wavelength. The effect of the developed algorithm in the JPN-48 model[2] as shown in **Figure 3 (b)**, which simulates a core network in Japan, is shown in **Figure 3 (c)**. One indicator of wavelength utilization efficiency is the maximum occupied wavelength number, which is the wavelength number occupied in the network. It has been confirmed to improve the maximum occupied wavelength number by over 20% by optimizing the use of this indicator and this algorithm. This shows that it is almost equivalent to the theoretical limit, without interrupting services.[3]

The developed algorithm is capable of relocation of optical wavelength resources in an arbitrary segment in the network. Applying this technology in particular to a segment in which traffic demand is high and wavelength resource depletion is significant is expected to be highly effective. That is, a service can be introduced simply by adding a transponder to an existing system without the need to install additional optical fiber. This allows optical network operators to effectively utilize the existing equipment and reduce capital investment as well.

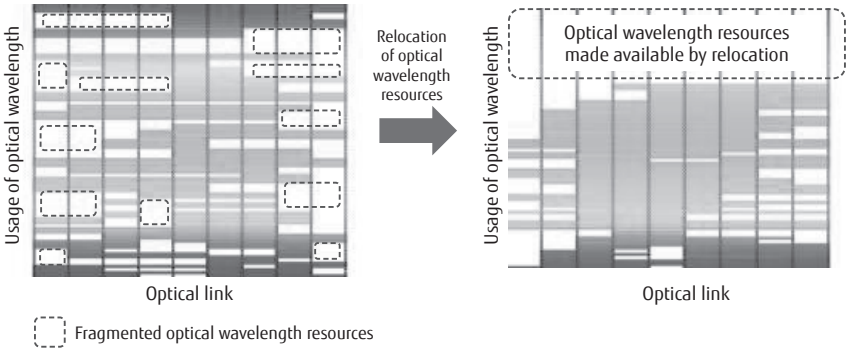
5.2 Self-diagnosis of IP networks

This section describes two issues and solutions for visualizing and monitoring network quality from the perspective of services:

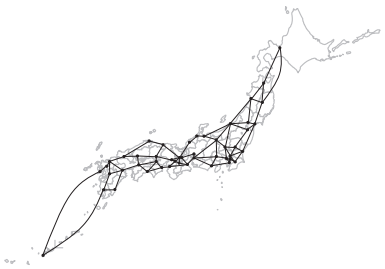
1) Network delay measurement and factor classification

Key performance indicators (KPIs) from a network perspective, such as packet loss and RTT, only allow network experts to find out how actual services are affected.

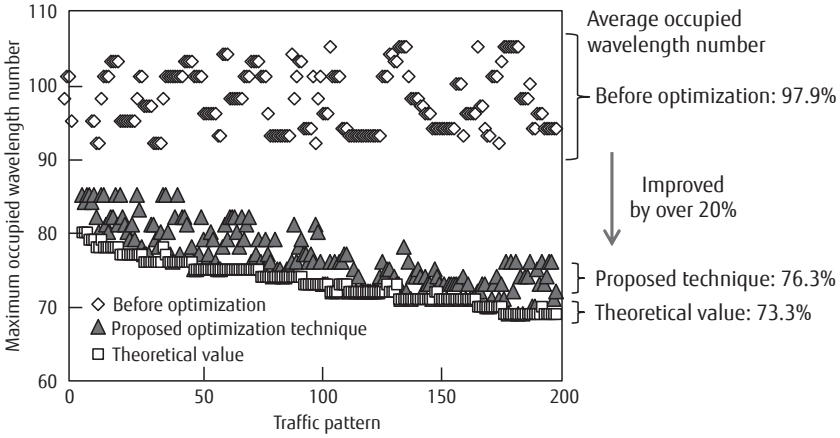
To deal with this issue, we have established a technique for classifying the measurement of the actual latency in responding to a service in the system into factors arising from network quality and from server and client processing (**Figure 4**). Specifically, latency has been classified into the following eight types.



(a) Fragmentation of optical wavelength resources



(b) Topology used for simulation (JPN-48 model)



(c) Effect of wavelength resource optimization

Figure 3
Optimization of optical wavelength resources in optical network.

- Connection establishment time
- SYN (connection request) retransmission time
- Client data transfer time
- Client data retransmission time
- Client processing time
- Server data transfer time
- Server data retransmission time
- Server processing time

In this way, detailed measurement of the latency itself that arises from network quality has allowed for the quantitative evaluation of the impact on actual services, which could not be grasped previously. Points that cause bottlenecks in quality improvement can also be isolated by classifying the factors. This allows problem points to be easily identified by non-experts of networks, who can now respond and formulate improvement plans. This technique does not depend on specific applications and can be applied to quality monitoring of various networks.

2) Establishment of error determination technique

The form of use of a network differs depending on the application, and the latency cannot be assessed with the same criteria.

To deal with this, we classified the latency in normal times measured in 1) classified for each application or subnet, and analyzed the standard deviation mean ± 3σ) of the latency distribution. Then, we established a technique which determines errors determination based on the change in the rate of exceeding the threshold covering 97 to 99% of the latency. With this technique, however, if the processing details differed for each application and variations in latency become large, common distribution models did not apply, which caused the error determination accuracy to decrease. To address this issue, we have applied a robust statistics-like technique.

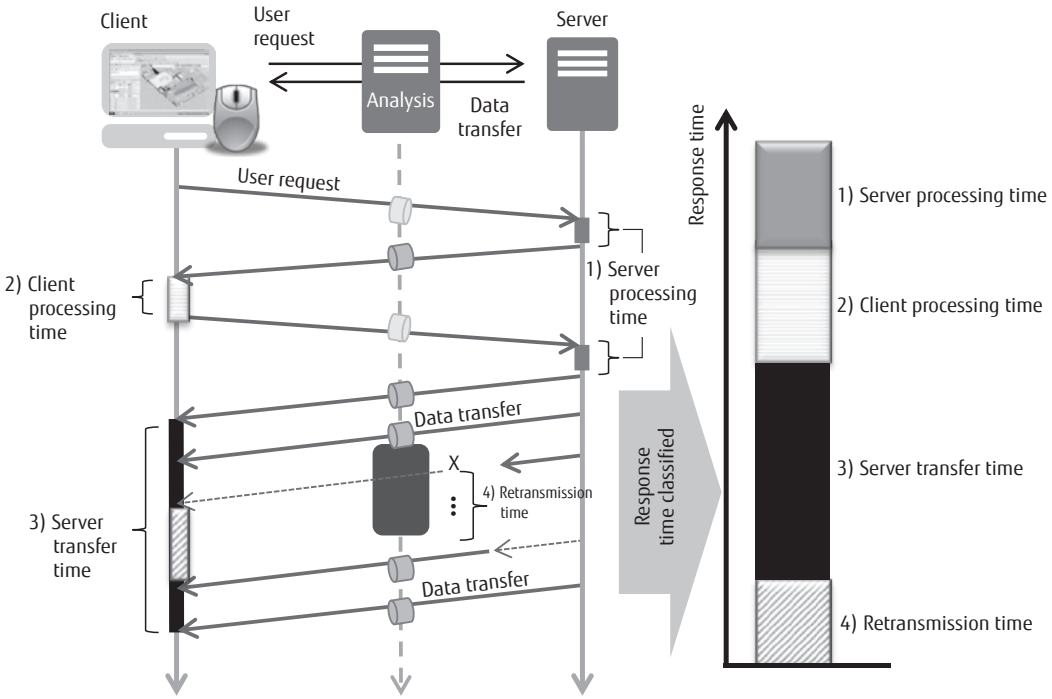


Figure 4
Quality analysis by response time.

While the median is often used as the representative value for data sequence containing outliers, it is not suitable for network KPI data, in which outliers frequently deviate to one side. For this reason, we have adopted the median absolute deviation (MAD) as an indicator that shows the spread of data using the trimmed mean. Then, the deviation from the distribution (standard deviation) is used as the threshold value to compare with the value in normal times. This has eliminated the need to set a threshold value for each application, allowing us to realize practical monitoring operations.

6. Conclusion

This paper described the early sign detection technology for preventing network failures and technologies for maintaining service quality developed by Fujitsu based on the concept of conscious network, which continuously provide services via networks.

These technologies are applied to optical and IP networks to realize integrated monitoring. This makes it possible to see if there is any impact on the packet layer (end-to-end) communication even if the optical layer has a problem, allowing end users to be notified. In the future, we intend to have the area of monitoring expanded to include data center fabric and wireless networks. While machine learning is utilized for some early sign detection of network failure, we plan to expand the scope of the application of AI technologies, including machine learning, to provide autonomous control at an earlier stage, thereby offering stable networks.

Part of this technology includes results from the "Research and Development on Elastic Optical Networking Technologies" entrusted by the National Institute of Information and Communications Technology.

References

1) Fujitsu: Fujitsu Accelerates Path to 5G and Conscious Networks with Next-Generation Variable Optical Transport. *http://www.fujitsu.com/us/about/resources/news/press-releases/2018/fnc-20180312.html*
2) Technical Committee on Photonic Network, The Institute of Electronics, Information and Communication Engineers: JPN Model.
3) Y. Takita et al.: Wavelength Defragmentation for Seamless Service Migration. Journal of Optical Communications and Networking,Vol.9,Iss.2, pp. A154–A161, (2017).

Takuya Nitta
Fujitsu Ltd.
Mr. Nitta is currently engaged in the development of packet analysis and accumulation products.

Yasuhiko Aoki
Fujitsu Ltd.
Dr. Aoki is currently engaged in research and development relating to network operation and monitoring technology.

Kyoko Ohya
Fujitsu Ltd.
Ms. Ohya is currently engaged in the development of network operation management products.

Fumiyuki Iizuka
Fujitsu Laboratories Ltd.
Mr. Iizuka is currently engaged in research and development relating to network service quality analysis technology.

Toshiki Honda
Fujitsu Ltd.
Mr. Honda is currently engaged in the planning and technology development of network operation enhancement solutions.