Network Sensing —Network Monitoring and Diagnosis Technologies—

● Masanobu Morinaga ● Yuji Nomura ● Takeshi Otani
● Motoyuki Kawaba

(Manuscript received April 7, 2009)

Problems that occur in the information and communication technology (ICT) systems (network services) deployed on Internet protocol (IP) networks may originate in the network, the servers, or even the data (content), which makes troubleshooting difficult and lengthens the time required for system restoration. In response to this situation, we have been developing monitoring and diagnosis techniques for network services based on the capture of packets flowing through the network. These highly sensitive techniques can detect problems that affect network service users and can quickly determine the cause and location of a problem without imposing an unnecessary load on the network. In this paper, we present a number of integrated monitoring and diagnosis techniques for network services that can be used to determine the causes and locations of network problems, diagnose server delays in services that span multiple servers, and detect sound-quality degradation in IP telephony services.

1. Introduction

IP networks such as the Internet and intranets have become indispensable elements of today's social and business infrastructure, and various ICT systems are operated on them. Since problems in ICT systems may lead to interruptions in business, maintaining a prompt response to such problems and an appropriate service level are important.

However, the services provided by ICT systems using IP networks (hereafter "network services") may encounter a type of failure known as a silent failure, which is not determined as an error by the system, or they may be subject to the simultaneous generation of large numbers of error logs. Therefore investigating the root cause may be complicated, with the result that identifying the cause and location of the problem is often difficult and time consuming. There are several reasons for this. One reason is that network systems do not directly monitor user traffic, and another reason is that it is difficult to diagnose whether the cause of a network service problem is in the network, or due to a shortage of server resources, or due to the content itself. Conversely, by implementing failure diagnosis based on the direct monitoring of user traffic, it is expected that system restoration from network service problems will be faster, and the service level will be also improved.

The authors of this paper have been working on the development of technologies for network quality management that are intended to support the stable operation of network services, and up to now we have engaged in research and development mainly on the network monitoring and diagnosis technologies that form the basis of the quality management technologies.

In this paper, with regard to the technologies for diagnosing the causes of network service problems, we will begin in the next section by introducing an approach to network monitoring

and diagnosis based on packet captures, to clarify the type of analysis. Following this, we will introduce a number of individual implementation technologies to analyze the causes of each respective problem.

2. Approach to monitoring and diagnosis

For monitoring and analysis with the objective of identifying the cause of a problem, statistical history information that can be acquired through management methods based on a common Management Information Base (MIB) alone is in many cases insufficient for analyzing the root causes of problems such as quality degradation.[1)] For more detailed analysis of the root causes of problems such as quality and performance degradation, it is important to analyze the detailed behavior of individual packets transmitted over networks (analysis of fields of IP, TCP, UDP headers, etc.). In the case of services such as IP telephony services, quality degradation inherent in the content (the audio signals transmitted/received as the payload) may be perceptible to the users, so the analysis of the content itself is also important. In this way, identifying the root causes of problems requires techniques that involve the analysis of entire transmitted packets. In this context, we have worked on an approach to monitoring and diagnosis of IP network services by capturing packets transmitted over networks.

Because many of the network services that need to be monitored and diagnosed are constructed in an open way in multi-vendor environments, it is difficult to understand their internal configuration and system behavior. As shown in **Figure 1**, the network services themselves are configured on tiers of system and service hierarchies, so problems with these services may have a number of different causes and locations. Accordingly, analyzing the causes

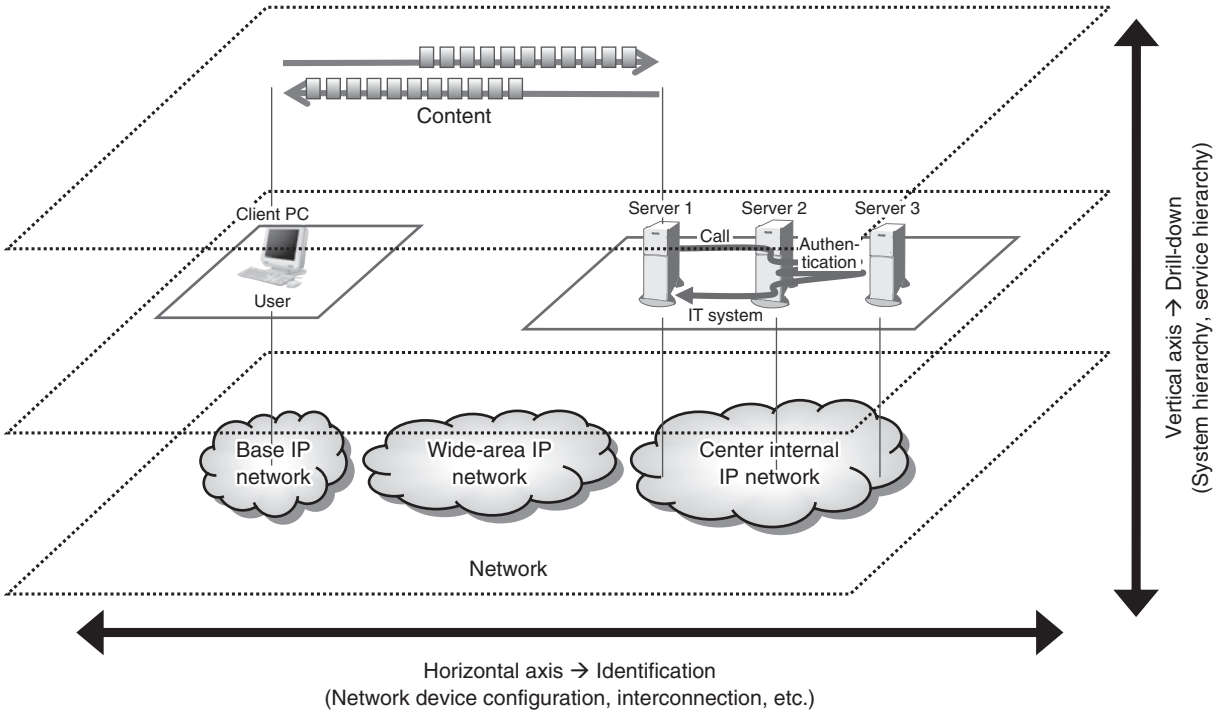


Figure 1
Approach for monitoring and diagnosis.

and locations of network problems requires a systematic analyzing technology by dividing the analysis into two components, namely, the horizontal axis, which is for identifying the location of the problem in the network configuration; and the vertical axis, which is for investigating the cause in more detail while drilling down[note)] the service and system hierarchies.

In the following sections, with regard to the diagnosis of the causes and locations of network service failure and quality degradation by means of capturing packets inside a network, we will first present technologies for identifying problems in networks and terminals/servers as the horizontal axis. After that, we will describe technologies for drilling down and diagnosing the causes of problems generated in terminals or servers as the vertical axis.

3. Identifying problems in networks

To enable recovery from a failure, both the location and the cause of the problem must be identified. This section presents several techniques that can be used to identify the location and cause of a problem in a network and explains the approaches to these respective techniques.

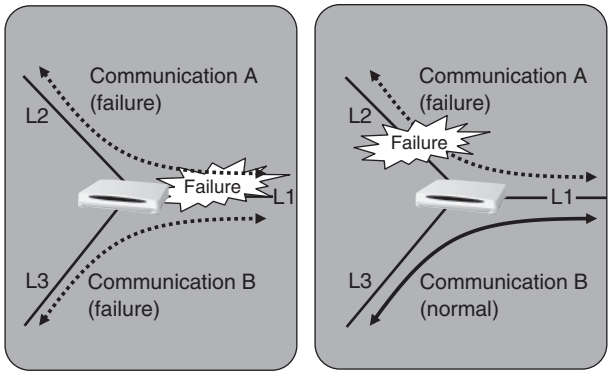
As a basic means of locating a problem, a technique called network tomography (hereafter "tomography") is common.[2)] This technique provides a method of locating a given failure based on a correlation between the network topology and whether or not any failure is generated in the communications passing through the network. This has the advantage of making it possible to locate a failure in a network where direct monitoring cannot be conducted. For example, it enables the identification of silent failures that are hard to discover using traditional device monitoring techniques based on MIB.

To give a simple explanation of the principle of tomography, suppose a case in which two communications A and B exist, where A passes through L1 and L2 and B through L1 and L3 (**Figure 2**).

If the same failure is detected in both communications A and B, the location of the failure is likely to be L1, a path shared by A and B [Figure 2 (a)]. Conversely, if a failure is detected only in communication A, the location can be inferred to be L2 [Figure 2 (b)].

This type of tomography is a widely known method. Traditionally, the most common solution was reduction to an optimization problem called a set covering problem, which has the disadvantage of making it hard to achieve sufficient computation speed and accuracy at the same time. We have developed a technology for using the relation of connections between links and nodes in a network, which is not used in conventional set covering problems. This only requires computation to trace the relation of connections for each node, in contrast to the conventional method computing for each link, and means that the failure can be located more quickly.

The technique described above allows real-time, high-accuracy locating of a failure even in a large-scale network with large volumes of traffic.



(a) L1 failure (b) L2 failure

Figure 2
Network tomography example.

note) To move from summary information to detailed data by focusing on the subject of analysis in order to identify the cause.

The next point is our study of the causes of problems. Problems in ICT systems including clients, networks, and servers can be roughly classified into performance problems and service outages. Of these, performance problems are generally caused by the following three phenomena.

1) Packet loss
2) Delay
3) Throughput reduction

While packet loss is generated mainly in networks, it may also cause delay or throughput reduction and so technologies that can accurately measure packet loss are extremely important. As a means to accurately measure packet loss, an advanced technology for accurately distinguishing packet loss from out-of-order packets, retransmission due to timeouts and failure to capture, etc., has already been developed. Regarding service outage, it has proven difficult to infer the root cause when the cause is a routing problem or an L2 loop. To address this issue, we have already developed a path visualization technology that uses Open Shortest Path First (OSPF) to obtain accurate routing information and a technology to accurately diagnose the loop location while a L2 loop occurs.

4. Identifying problems in a network and client/server

Applying tomography as described in the previous section makes it possible to identify where a problem exists between a client/server and a network. For example, in Figure 2 (a), if L2 and L3 are on the same subnet and are each connected by a single terminal, the problem can be assumed to be in L2 or the terminal. If the cause is delay or throughput reduction rather than packet loss, the terminal can be presumed to be the cause because the probability of these causes is low in local area networks. In reality, however, not all topologies are simple enough to allow identification as in Figure 2 (a). If the topology is unknown and the cause of the problem is a delay, both the network and the terminal are possible locations of the cause, which makes identification difficult. Accordingly, we have developed a technology to measure the delay time for each layer. Specifically, the delay in a lower layer is measured, such as an ACK response to TCP data, which is unlikely to be affected by a terminal or application delay. Similarly, the delay is measured for a request and response on layer 7, such as HTTP, in which an application delay is reflected. Using these two delay measurement technologies, the cause of the delay can be assumed to be in the network when the delay on the lower layer is constantly large, thereby enabling highly accurate identification.

The causes of the performance problems that show up as throughput reduction phenomena are mostly the effects of TCP window flow control due to an increased delay or because of insufficient effective network bandwidth. In either case, the cause is presumed to be in the network and the abovementioned delay measurement technologies allow the cause to be identified as either a delay or bandwidth insufficiency.

5. Drill-down of problems in servers

Slower processing in a server may be perceived by users as a network service delay when no network delay occurs. In order to pinpoint the cause and location of a system slowdown, it is essential to analyze both the network delay and the server processing time. In general, it is not a simple task to measure the processing time of an individual server. In a simple client-server system configuration, the time a server spends in the processing of a network service can be determined by simply subtracting the network delay from the network service delay, that is, the roundtrip delay of a user's request. However, in a commonly used multi-tier system (a three-tier system including Web servers, application servers and DB servers, for example), the processing time of the individual

servers must be determined taking into account the invocation path along which the servers' operations are processed across the system.

For this reason, we have developed a technology[3] to detect the invocation path of each service processing, and calculate the processing time of the individual servers via a more detailed analysis of the packets exchanged between them (**Figure 3**). Primarily, this technology identifies each invocation path by recognizing the sequence of messages flowing through multiple servers to process a service, referring to predefined appearance patterns of the messages contained in the packets. Combining this sequence recognition with TCP sequence analysis allows computation of the processing time of each server. Thus, this technology can identify the location of a network service delay across multiple servers.

6. Drill-down of problems in content

In recent years, the telephony services provided on IP networks (IP telephony services) have become widespread. In IP telephony services, users experience network service quality (speech quality in this case) in real time. The speech communication quality of IP telephony services consists of the quality of the network such as packet loss and the quality of the content (audio signal) itself.[4),5)] It is possible to use the aforementioned method of detecting a failure and identifying its cause/location to detect the causes of degradation of network quality. However, there were no adequate methods to detect degradation of an audio signal.

Accordingly, a novel acoustic signal processing technology is developed, in which cause-specific degradations of audio signal are detected by analysis of the digital speech payload of captured packets. Since echoes and noise are reported as dominant degradation factors of speech communication quality, the technology aims to detect echoes and noise by processing signals. An echo is a reflection of the speaker's own voice and comes back to the speaker as an annoying received sound. And it can be detected

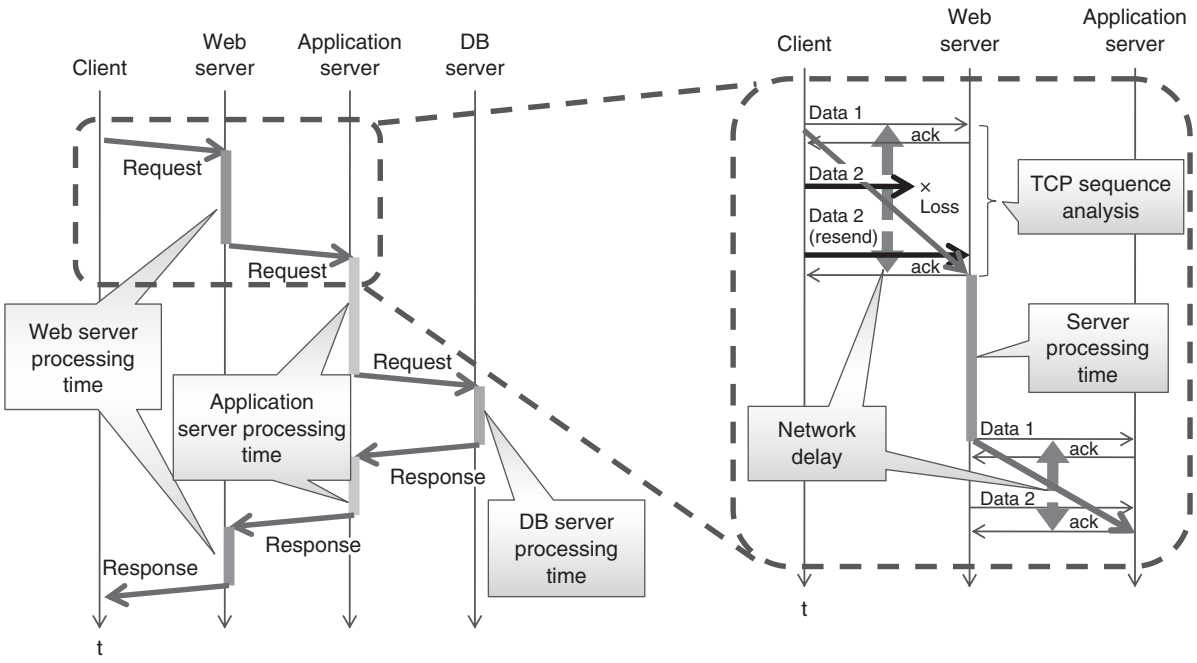


Figure 3
Analysis of request/response messages among multiple servers.

by using acoustical similarities between the transmitted signal and received signal. However, to detect an echo precisely, interferences with the other party's voice and background noise in the echo detection should be taken into account. Therefore, our technology specifies the frequency bands in which the interference is comparatively low, and evaluates similarities only in these bands so as to avoid incorrectly detecting echoes. In addition, there is no method to detect unnatural noises caused by problems with the network appliance. Particularly there is a demand to detect a pulse noise caused by inadequate connection of a circuit and a humming noise resulting from electromagnetic wave interference generated in the power supply circuit. Therefore we have also developed a technology to detect the pulse noise and the humming noise by time-frequency domain analysis of an audio signal.

For the acoustic analysis, the preprocessing of captured packets prior to analysis is important. Echo analysis requires preprocessing that groups incoming and outgoing packets into pairs of time-series data. However, RTP sessions, which transmit content, may contain non-audio signals such as Dual-Tone Multi-Frequency (DTMF) signals as well as audio signals. Thus, analyzing the signals as a mixture of audio signals and non-audio signals may generate a time-series displacement of pairs of incoming and outgoing packets. As a result, this may lower the accuracy of detection. To address this problem, we have developed a filtering technology that performs real-time separation between audio and non-audio signals at the time of capturing packets, and synchronizes and extracts the pairs of incoming and outgoing time-series data.

Combining the aforementioned technologies for monitoring IP phone networks enables network administrators to acquire information in real time about the degradation of speech on a cause-specific basis, and as a result, administrators may be able to promptly respond to problems.

7. Conclusion

In this paper, as monitoring and diagnosis technologies, we have introduced approaches to a number of technologies for systematically diagnosing the causes of problems in network services based on packet capture.

Networks are projected to continue increasing in terms of complexity and sophistication, while the terminals connected to these networks and the services configured across entire networks are also expected to undergo further diversification. In addition, these diversified services will result in a dramatic increase in the volume of traffic handled by networks. The systematic technologies for diagnosing the causes of problems presented in this paper are considered to have the potential to provide a strong foundation that can be applied to these future networks. From now on, in the interests of monitoring and diagnosis of future networks, which will be developed constantly while becoming more sophisticated and diverse and increasing in capacity, we intend to continue our research on the development of new technologies that include further increasing the speed and capacity of processes and the control of autonomous quality management by networks themselves.

References

1) Satoshi Nojima et al.: Health-Care Technology for Networks—Autonomous and High-Availability Network. (in Japanese), *FUJITSU*, Vol. 56, No. 4, pp. 313–318 (2005).
2) Toru Hasegawa et al.: Measurement Techniques for Quality and Failure Location over Large Scale Networks. (in Japanese), *The Journal of the Institute of Electronics, Information, and Communication Engineers*, Vol. 91, No. 2, pp. 92–97 (2008).
3) Riichiro Take: Real-time System Behavior Visualization Technology for Managing Complex Distributed Application Systems. (in Japanese), *FUJITSU*, Vol. 59, No. 1, pp. 33–38 (2008).
4) TTC: JJ-201.01 "A Method for Speech Quality Assessment of IP Telephony (5th Edition)". (in Japanese), August 2008.
5) ITU-T Recommendation G.107 (05/2000): The E-model, a computational model for use in transmission planning.

Masanobu Morinaga
Fujitsu Laboratories Ltd.
Mr. Morinaga received B.E. and M.E. degrees in Electronic Engineering from Kyushu University, Fukuoka, Japan, in 1991 and 1993, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1993, where he has been engaged in research and development of network operations and management systems. He is a member of the Information Processing Society of Japan.

Takeshi Otani
Fujitsu Laboratories Ltd.
Mr. Otani received B.S. and M.S. degrees in Electronic Engineering from Hokkaido University, Sapporo, Japan in 1998 and 2000, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 2000, where he has been engaged in research and development of speech enhancement algorithms and speech communication systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Yuji Nomura
Fujitsu Laboratories Ltd.
Mr. Nomura received B.E. and M.E. degrees in Information Engineering from Hokkaido University, Sapporo, Japan in 1992 and 1994, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1994 and has been engaged in research and development of enterprise network management systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Motoyuki Kawaba
Fujitsu Laboratories Ltd.
Mr. Kawaba received an M.E. degree in Information Engineering from the University of Tokyo, Tokyo, Japan in 1991. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1991 and has been engaged in research and development of performance modeling and analysis of wide-area distributed systems.