Improving IP-based OSS Reliability During Large-scale Disasters

DOCOMO Technology, Inc., Solution Service Division
Hideki Kitahama
Takefumi Nagasawa†
Susumu Nishio
Tomoyuki Otani

The IP-based Operation Support System (OSS)*1 monitors the large-scale routers and switches that form the backbone IP network and also monitors pieces of peripheral IP network equipment that carry communications via these routers and switches. This is a large-scale monitoring system that covers approximately 30,000 units. As shown in **Figure 1**, the old IP-based OSS was a dual-system redundant

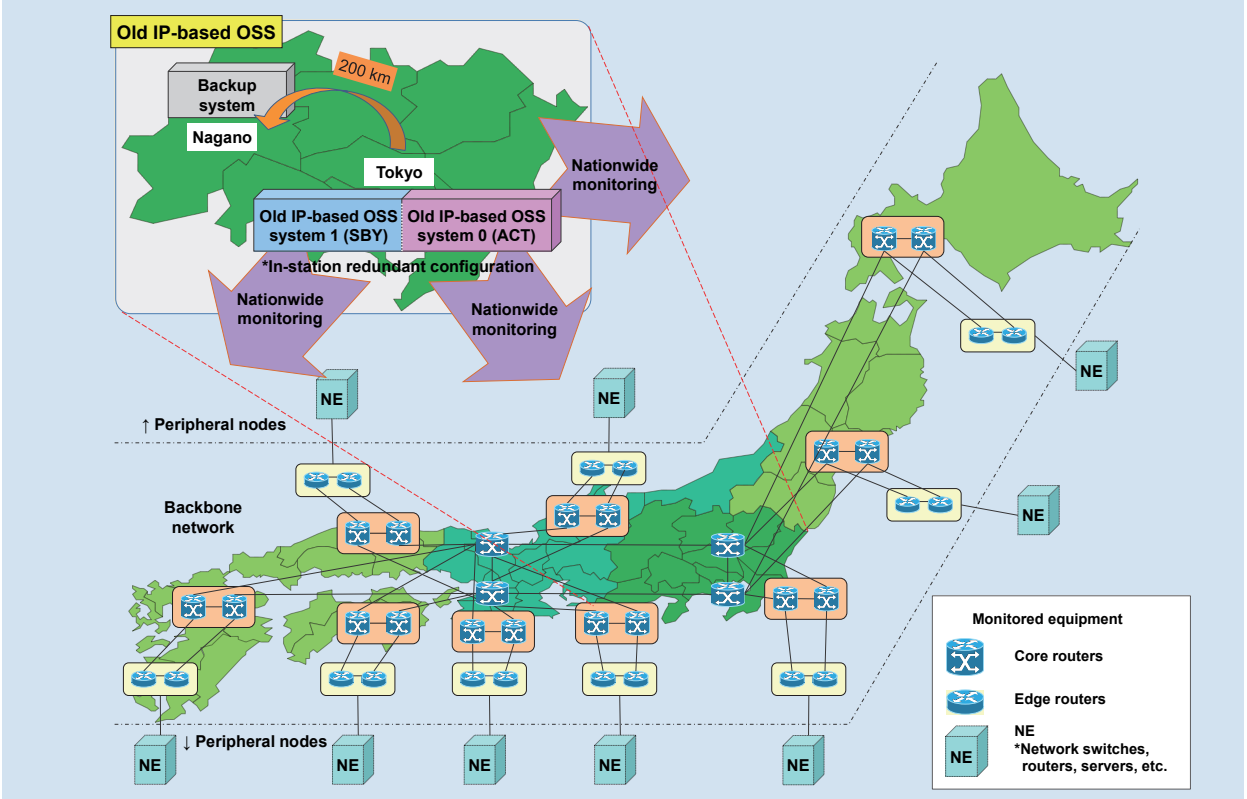

Figure 1 Old IP-based OSS monitoring system configuration

† Currently DOCOMO CS, Inc., Solution Integration Department

*1 **OSS:** A system for discovering failures and congestion in the mobile communications network and performing appropriate control functions or measures in response to such problems.

configuration located in a building in Tokyo for monitoring nationwide Network Elements (NE)*2 with Simple Network Management Protocol (SNMP)*3/Syslog*4. In addition, a third backup system was set up in Nagano that could be manually switched on if the two Tokyo systems simultaneously failed.

The OSS had continued stable operation without major malfunctions that disabled monitoring since its introduction in 2002. Therefore, it was considered that the OSS had thorough disaster countermeasures. However, due to the Great East Japan Earthquake of 2011, it became necessary to assume two new potential scenarios, since the impacts of that disaster were more far-reaching than anyone had expected.

(1) In the first scenario, since Tokyo and Nagano are only 200 km apart, in the worst case both bases could be destroyed. Also, even if the Nagano backup system survived the direct impacts of a disaster, ensuring availability of maintenance personnel would be difficult due to lifeline and transport paralysis, meaning systems launch would be greatly delayed (**Figure 2** (a)).

*2 **NE:** A functional block that achieves a necessary function in the provision of telecommunication services. Specifically, a unit of telecommunication equipment such as a switch, transmitter or radio station.

*3 **SNMP:** Protocol for communicating information for monitoring and controlling network equipment on IP networks. Can receive TRAP and acquire MIB information.

*4 **Syslog:** A protocol for recording system operation conditions and error messages and exchanging the data with other computers via a network.

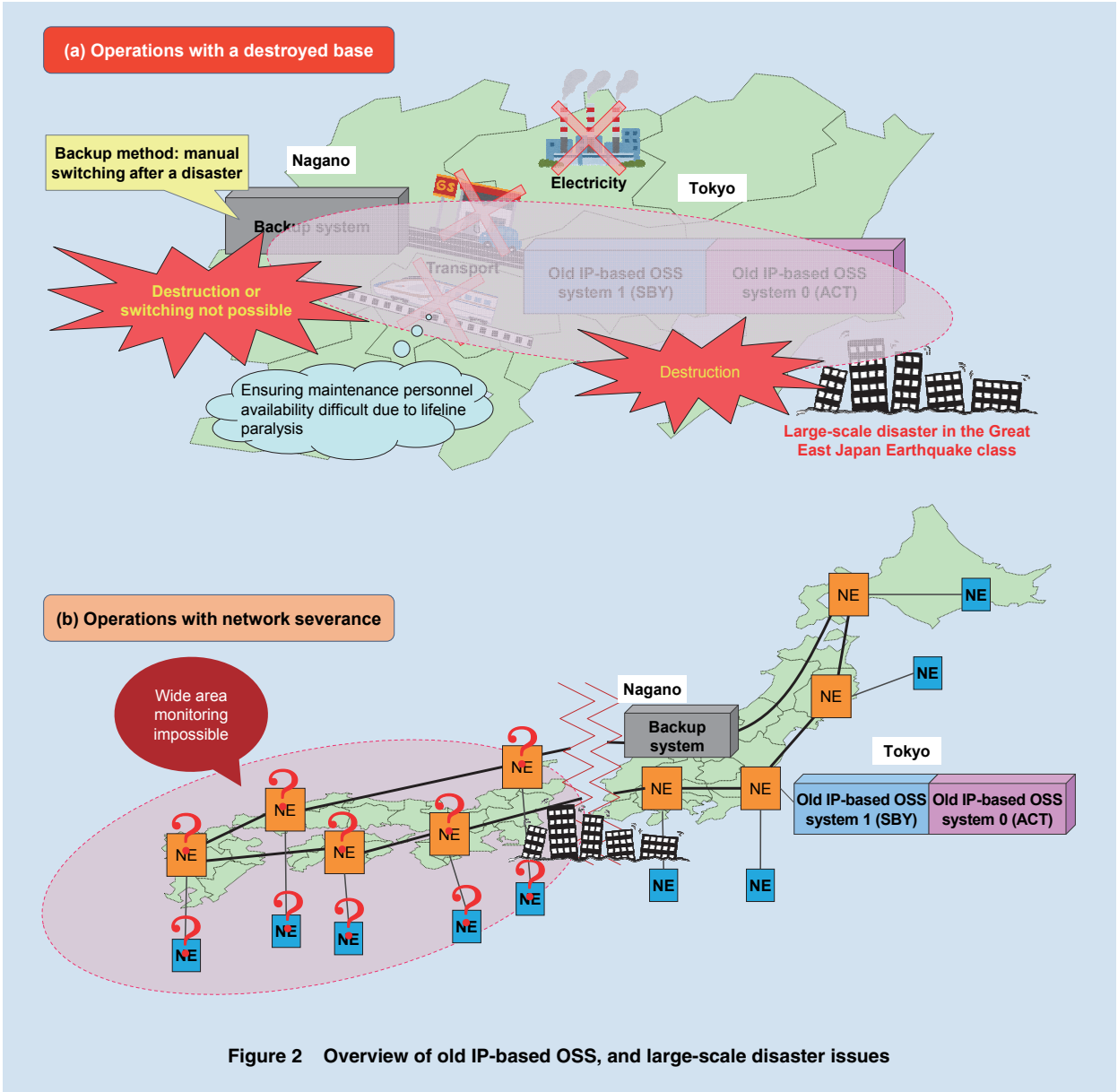

Figure 2 Overview of old IP-based OSS, and large-scale disaster issues

(2) In the second scenario, network transmission paths on networks accommodating NE nationwide could be severed. In this case, it would be impossible to monitor NE beyond the point of severance, and hence the affected areas would be extremely large (Fig. 2(b)).

Since these conventional backup systems are costly because they require the hardware resources of a whole extra system even though they are not operational during normal times, and since their operation cannot be satisfactorily guaranteed in times of large-scale disasters, NTT DOCOMO decided to shift to new IP-based OSS with advanced disaster resilience. The new IP-based OSS are designed to enable discontinuance of high-cost backup systems while enabling building of low-cost redundant systems in locations that are far apart so that they are not affected by the same disaster, without increasing the number systems. As shown in **Figure 3**, the StandBY (SBY) system has been moved to Osaka, where a 24-hour maintenance system can be established to enable remote redundancy between Tokyo and Osaka by adopting a 2-base, 1-system configuration where two systems can be operated simultaneously [1].

Figure 4 shows the structure and operation of the new IP-based OSS compared to the old system. With the new IP-based OSS, a remote cluster is formed from the two systems with a dedicated broadband network (several tens of Gbps) between the bases in Eastern and Western Japan. This enables messaging between the two systems including keep-alive*5, and database synchronization to achieve redundancy of the two systems (Fig. 4, top).

In normal times, the bases in Eastern and Western Japan operate as ACTive (ACT)/SBY*6 (strictly speaking, ACT/SBY is switched for individual functional servers, however, for brevity, this description assumes that all functional servers are switched over to one base). NE are set to always send monitoring messages to the systems in both bases, and consideration has been given so that in any condition, no monitoring messages are lost, even in the routing chaos right after damage has been caused by a disaster (**Figure 5**). These monitoring messages from NE are processed at the ACT side, and the results of processing are synchronized with the

*5 **Keep-alive:** Communications performed periodically to confirm the validity of connections between devices on a network.

*6 **ACT/SBY:** A system configuration in which two servers perform the same function with one server in active mode (ACT) and the other in standby mode (SBY). Service interruptions are prevented by immediately continuing operations on the SBY server whenever a fault occurs on the ACT server. The SBY server is always kept in the same state as the ACT server during normal operations in preparation for switching.

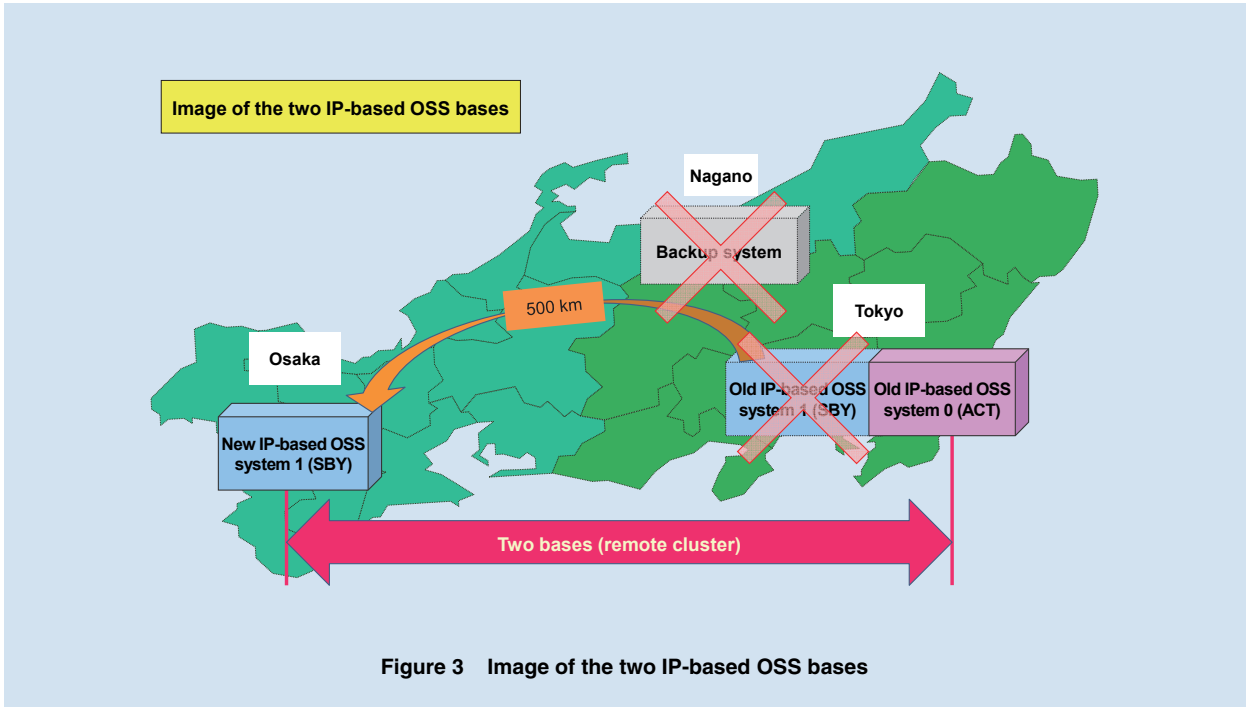

Figure 3 Image of the two IP-based OSS bases

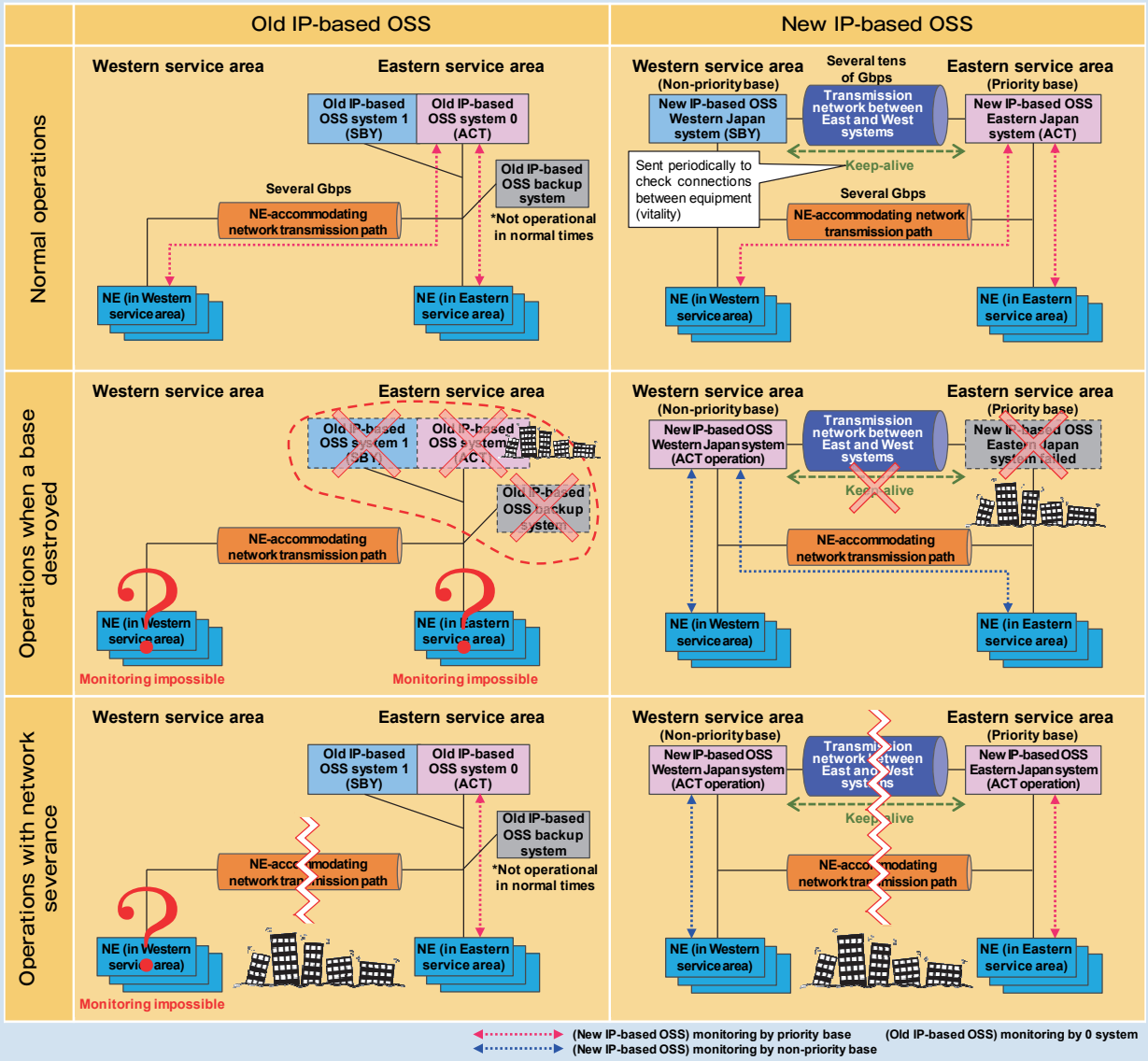

Figure 4 Configuration of old and new IP-based OSS systems and operations with disasters

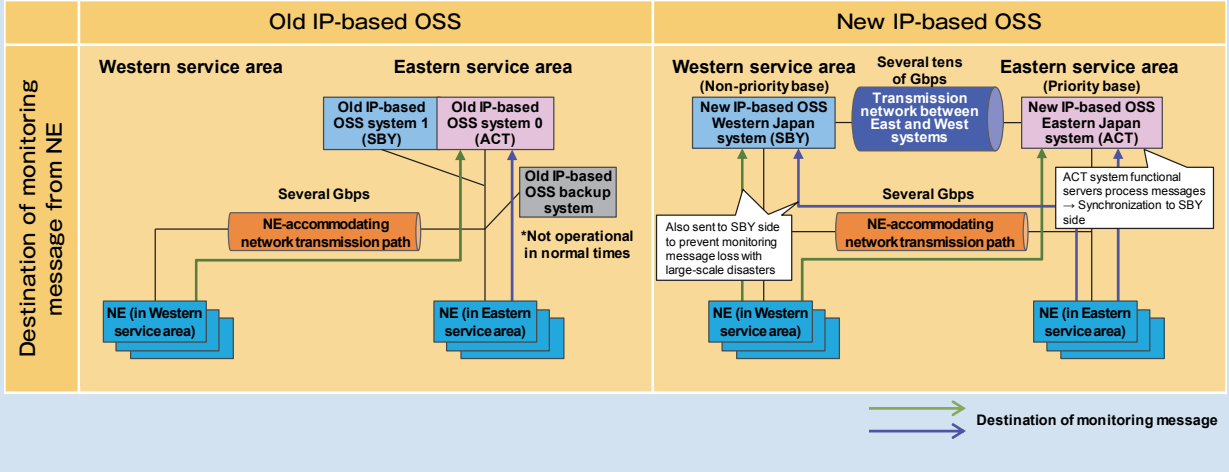

Figure 5 Sending monitoring messages from NE to the old and new IP-based OSS

SBY side.

(1) In the first scenario, if a base is destroyed due to a large-scale disaster, the old IP-based OSS is no longer able to monitor. However, with the new IP-based OSS, if keep-alive between ACT and SBY cannot be received, the SBY side immediately switches to ACT and continues monitoring (Fig. 4 center).

(2) In the second scenario, if the communications network between the bases in Eastern and Western Japan is severed, the old IP-based OSS will no longer be able to monitor NEs beyond the severance point. However, if the new IP-based OSS fails to confirm the vitality through keep-alive, the SBY system in Western Japan commences ACT operations, and since both systems are now operating in ACT, monitoring of nationwide NE can continue. Since the network between Eastern and Western Japan is completely severed, the systems in Eastern and Western Japan can only monitor NE under their respective service areas (Fig. 4, bottom).

Introducing simultaneous ACT operations in both bases has also brought about new issues. With operations in a network severance scenario with the new IP-based OSS, if some networks accommodating NE are lucky enough to survive the severance, that NE will be double monitored via both systems, which will increase monitoring processing load (**Figure 6** (a)). Here, although there were no significant impacts on most of the equipment, serious impacts were seen in ultra-large-scale routers with their vast number of monitoring points, preventing normal operations. Hence, attention is required as there is a tendency to think that ultra-large routers have spare processing capacity. In response to this issue, functions were added to the new IP-based OSS, so that when the system switches from SBY to ACT, vitality confirmation is performed via NE-accommodating networks just in case, and if ACT is detected at both bases simultaneously, then monitoring of double monitoring non-permissible NE is stopped at the non-priority base side (Fig. 6 (b)).

This article has described new IP-based OSS configuration and operations. The system was implemented and started commercial operations in

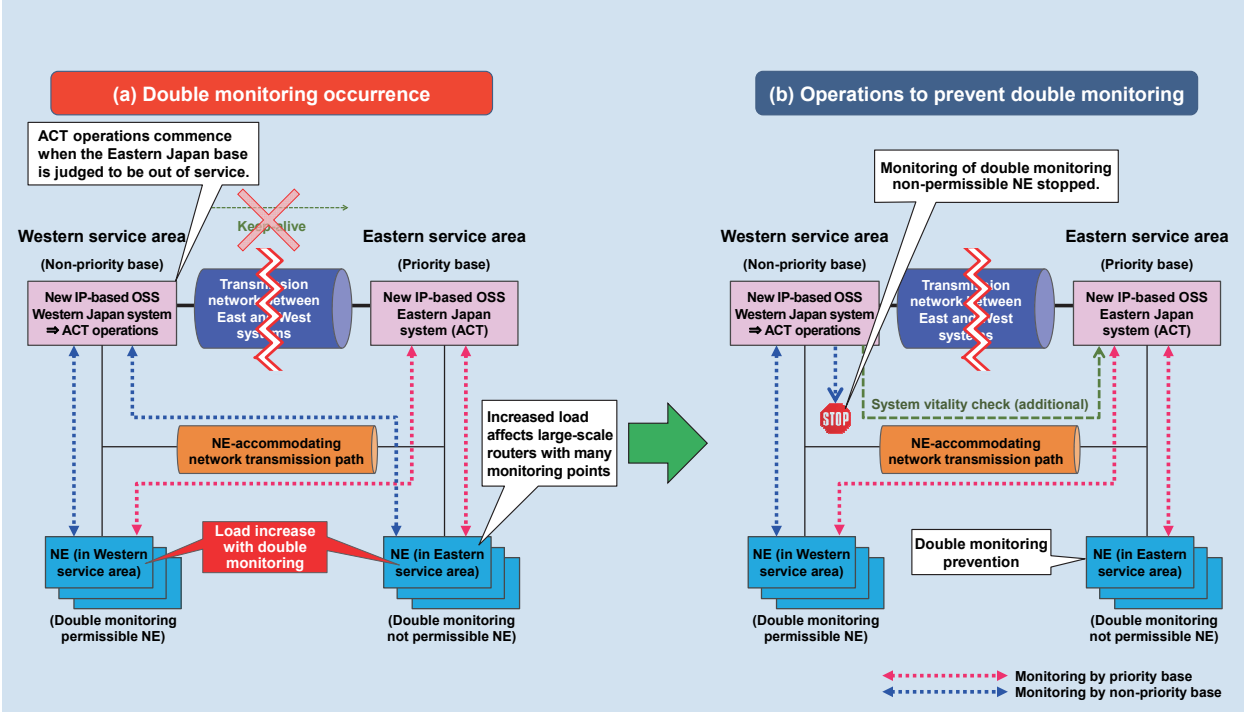

Figure 6 Operations to prevent double monitoring with new IP-based OSS

February 2016, and promises stable monitoring even at the time of large-scale disasters. As a future issue, we would like to automate some aspects of the database merge processing following elimination of simultaneous ACT operations in the two bases, which currently have to be done manually.

Reference

[1] K. Takahashi: "Economical OSS against a Great Earthquake," Institute of Electronics, Information and Communication Engineers, Technical report, Vol.112, No.392, NS2012-151, pp.61-66, Jan. 2013 (In Japanese).