SYSLOG | Commodity IP Equipment | Malfunction Detection

Assistant System for Detecting Potential Malfunctions in Commodity IP Equipment

DOCOMO Technology, Inc. Radio Network Division
Atsushi Tsuyuki, Mitsuru Shimizu
Naoto Shimada and Syunsuke Iwamoto

1. Introduction

With the increased traffic of recent years, the demand for high-capacity network equipment is on the rise. NTT DOCOMO is continuing to increase the capacity of the communications equipment on our communications network. However, these upgrades also bring more potential for adverse effects on users if malfunctions occur, and hence require greater levels of preventative maintenance. Adding to this challenge, commodity IP equipment has many limitations in terms of maintenance and monitoring compared to custom-designed equipment, detailed information on functionality of a range of components is not available, and there are no standardized methods for quickly analyzing the causes of malfunctions.

To counter these issues, DOCOMO Technology was asked by NTT DOCOMO to develop a system to expand maintenance and monitoring of commodity IP equipment, thus, we developed this system to reduce adverse effects on services by enabling early analysis of malfunctions when they occur, and detection of latent malfunctions before they surface.

Using our know-how in handling equipment, acquired through testing commodity IP equipment and deployment support etc, we developed a lower cost system than other similar existing systems, by implementing only the minimum functional requirements. We also developed this system using the agile development method to include the many detailed demands of network maintenance staff.

This article describes an overview of the system we developed for detecting potential malfunctions in commodity IP equipment.

2. System Requirements

Below is a list of functions network maintenance staff asked to be included in this development.

- Support all IP devices implementing syslog*1.
- Network monitoring from PCs (in offices) connected to in-house LAN.
- Free monitoring of any station and event.
- Active alert notifications.
- Ability to display Station Name and Event Details in log messages in non-alphanumeric characters.

3. System Overview

This system is designed to assist monitoring of networks through existing network monitoring systems, and aims to enable early detection of troubles and swift uncovering of malfunction causes by analyzing syslog messages that arise from commodity IP

*1 **syslog:** A standard used to transfer log messages on IP networks.

equipment operations, and also aims to enable detection of potential malfunctions. The system automatically and periodically collects logs from the syslog server that collects the syslog messages output by the commodity IP equipment in HyperText Transport Protocol (HTTP)*2. If a message about an anticipated malfunction is output, the system notifies network maintenance staff.

The relationship between this system and existing network monitoring systems is described below. Commodity IP equipment on the DOCOMO network is monitored using a network monitoring system called "IP-Management Tool" (IP-MT), which is used for monitoring and maintaining all IP equipment installed on the DOCOMO network from a common standpoint. IP-MT analyzes Simple Network Management Protocol (SNMP)*3, TRAP*4 received/Management Information Base (MIB)*5 information acquired, and partial syslog messages to perform monitoring (monitoring is limited to prevent network or system overload if the number of messages output increases too much).

This system enables maintenance staff to freely set conditions to filter stations and syslog messages to sort out objects to be monitored. In this way, this DOCOMO network monitoring assistance system aids the early discovery of problem events (**Figure 1**).

The system characteristics are as follows:

- In addition to the OPeration System (OPS)*6 network connection functions, the inclusion of in-house LAN connection functions enables monitoring from an office.
- The inclusion of functions that enable maintenance staff to freely specify stations and messages enables greater maintenance and monitoring accuracy.
- The system alert notification functions (minimum every minute) makes it easier to understand when malfunctions occur.
- A find-and-replace function lets maintenance staff freely replace IP addresses and the body of messages in messages output with character strings, to quickly and easily pinpoint stations and find out message details.
- Setting conditions linked to past malfunction and syslog output situations enables quicker detection of similar events and raises the accuracy of event prediction.
- Easy customization enables support for all IP equipment implementing syslog, from the Radio Access Network (RAN)*7 routers, through to

*2 **HTTP:** A communications protocol used to send and receive HTML and other content between Web browsers and Web servers.
*3 **SNMP:** Protocol for communicating information for monitoring and controlling network equipment on IP networks. Can receive TRAP and acquire MIB information.
*4 **TRAP:** Notifications actively transmitted from IP equipment to servers.
*5 **MIB:** Database for managing devices installed in IP equipment.
*6 **OPS:** General name for systems used for maintaining and operating communications networks.

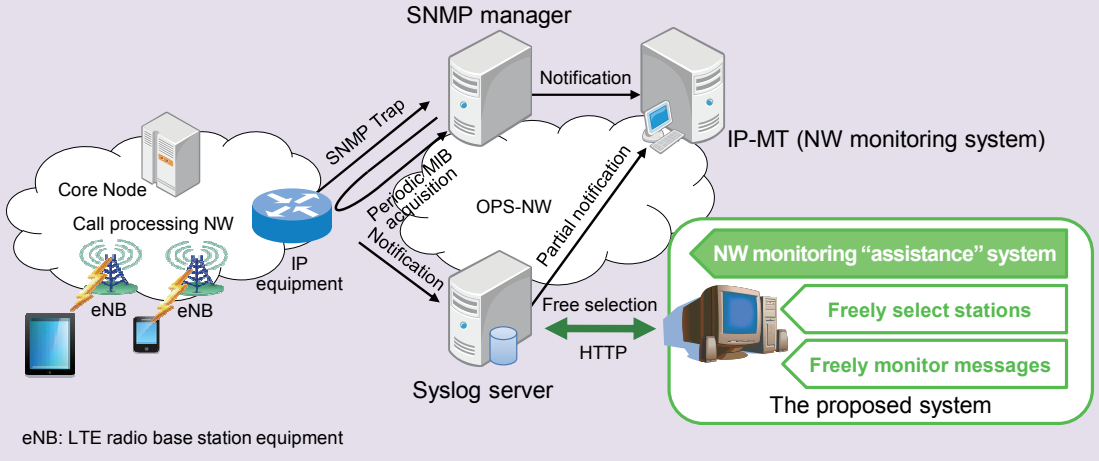

Figure 1 Relationship with existing monitoring systems

Core Networks (CNs)*8 and OPS.

Table 1 lists maintenance staff PC requirements for operating this system.

4. System Functions

System functions are shown in **Figure 2**. The system consists of (1) NW connection, (2) Condition settings, (3) Log find-and-replace, (4) Output, (5) Syslog file read and (6) Telnet *9 functions.

To monitor IP devices connected to the network, maintenance staff can select methods to suit their purposes, based trends in error occurrence from past logs etc. This article describes functions (1) to (4) - the functions characteristic of this system.

(1) Network Connection Functions

This system has two types of network connection functions - "Direct Monitoring" and "Folder Monitoring (**Figure 3**)."

- Direct monitoring

  A simple connection method for monitoring using HTTP to connect this system (PCs) on OPS network directly to syslog servers. This is a network monitoring method using this system that enables monitoring mainly done by networks operation center supervisors etc who always work with monitoring systems on OPS networks in parallel with usual IP-MT monitoring work.

- Folder monitoring

  This is a method of monitoring folders that store syslog files created in file servers from this system (PCs) via an in-house LAN network. Using existing facilities installed on OPS networks and in-house LAN enables monitoring from an

*7 **RAN:** General name for communications networks accessed via radio.
*8 **CN:** The core network of a communications network.
*9 **Telnet:** A virtual terminal software and protocol that enable remote operation of servers from a local computer on a TCP/IP network.

Table 1 System requirements

OS		Microsoft Windows® 7
Platform		(1) Microsoft®.NET Framework 3.5 (2) Microsoft® Chart Library 3.5
PC performance	CPU	A PC Intel Core 2 Duo (1 GHz) or greater on which the above Japanese version OS will run.
	Memory	1 GB or more
	HDD	Main: 10 MB or more Log storage area: 5 GB or more recommended (will decrease or increase depending on log storage period).

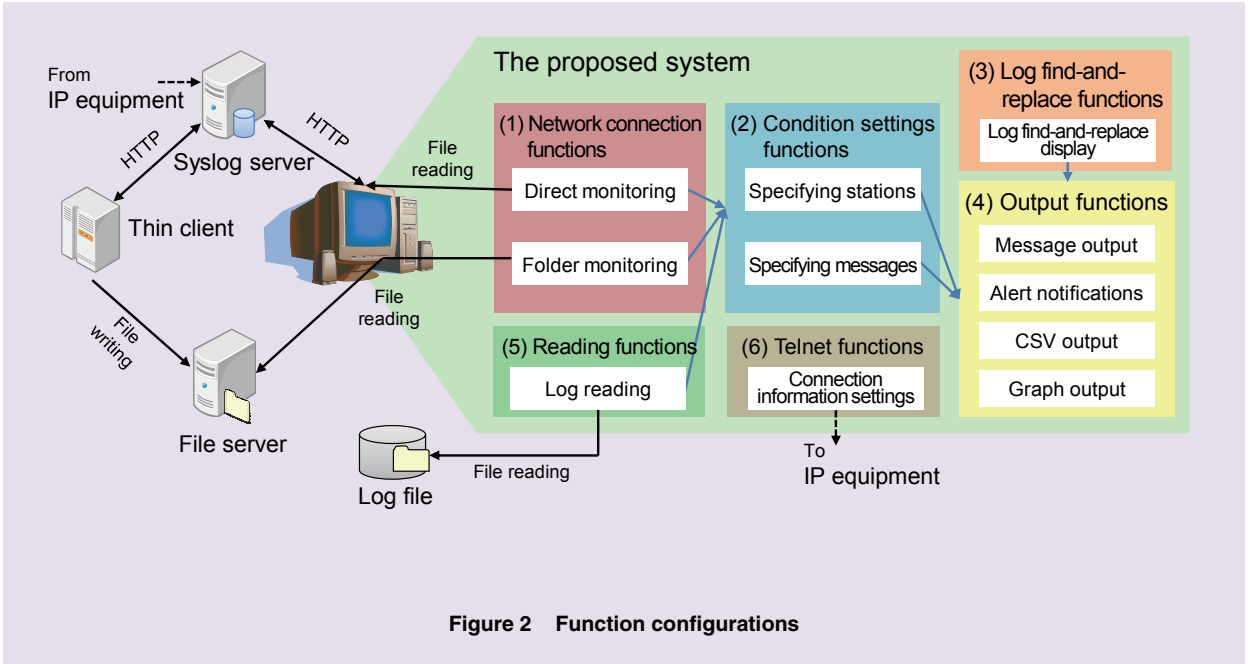

Figure 2 Function configurations

office from this system (PCs) on an in-house LAN, by acquiring syslog information.

Syslog files are periodically acquired through thin clients (existing OPS network facilities) installed on OPS networks, through HTTP connection to the syslog server. Acquired syslog files are stored in a file server (existing in-house LAN facility) on the in-house LAN, and are updated when syslog files are periodically acquired. Using existing facilities enables a connection system that needs no extra facilities on the OPS and in-house networks, which enables supervisors to monitor specific malfunctions from their offices.

(2) Condition Settings Functions

This system has functions that enable network maintenance staff to specify messages or stations to be monitored, so that alerts (described later) will be output. These functions enable quicker confirmation of malfunctioning stations or malfunction events because they can be used to sort out specific stations or events for monitoring. Furthermore, by limiting monitoring to certain stations or events, the message processing load on the system is minimized, which enables monitoring to be performed without overload (**Figure 4**).

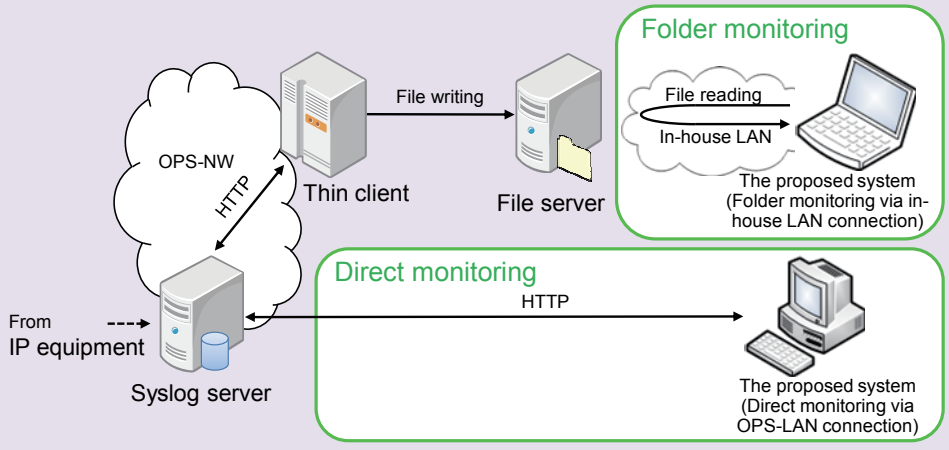

Figure 3 NW connection functions

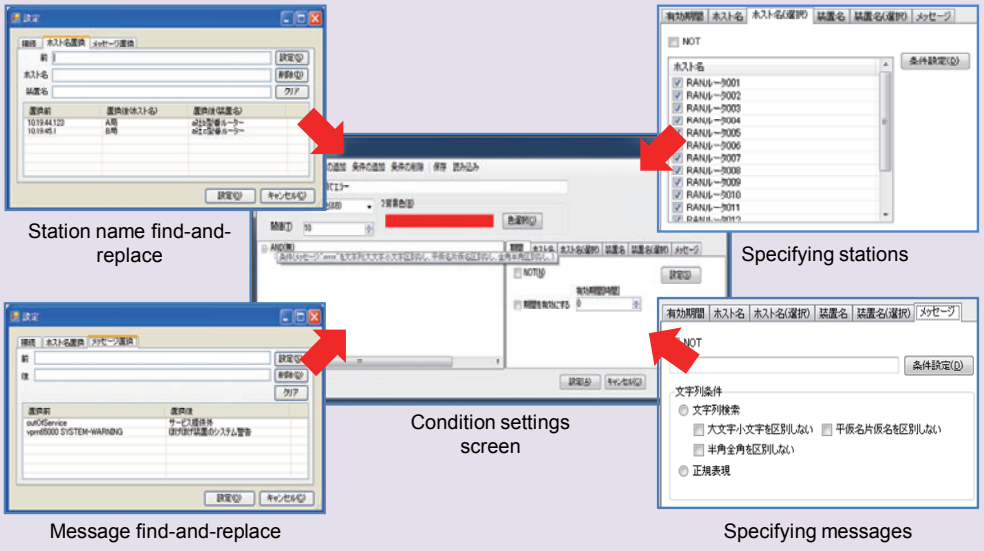

Figure 4 Condition settings screen

(3) Log Find-and-Replace Functions

This system has a log find-and-replace function that enables network maintenance staff to freely find and replace IP addresses and output messages with specific character strings (station name, event details etc). This function enables automatic linking of IP addresses with station names, or messages with events, which will reduce the time taken to perform counter-measures once a malfunction occurs (**Figure 5**).

(4) Output Functions

These functions notify network maintenance staff of data extracted that meets specified conditions (alert outputs), and also output information in various formats for different purposes (extracted syslog messages, graphs depicting the frequency of occurrence or CSV*10 format). The functions can raise monitoring accuracy and network quality by enabling analysis of malfunction trends, quick confirmation of messages and monitoring while performing other work (**Figure 6**).

5. Conclusion

This article has described an overview of a system we developed to assist existing monitoring

*10 **CSV:** "Comma Separated Values" - A text data file format that contains text data separated by commas (",").

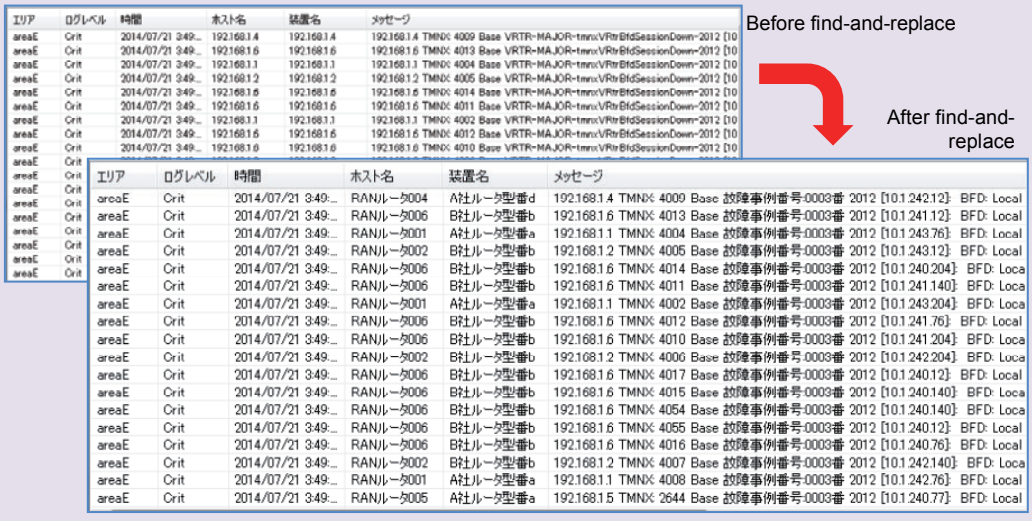

Figure 5 Message output examples

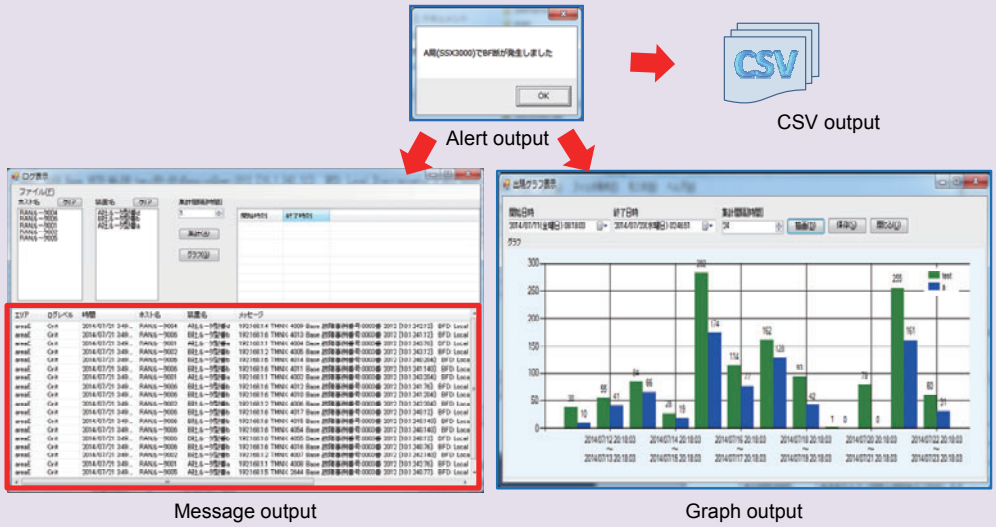

Figure 6 Output examples

systems for maintaining and operating commodity IP equipment in RAN environments.

As well as supporting stable operation of IP equipment and DOCOMO communications networks, this system enables quick and flexible response with addition and improvement of functionality, and can be widely used to quickly and accurately uncover potential malfunctions across an entire network, including malfunctions in RAN IP, CN IP or OPS IP equipment, and thus raises the quality of the network.