A Cooperative LAN Diagnostic and Observation Expert System

Toshiharu Sugawara
NTT Software Laboratories
3-9-11, Midori-cho, Musashino-shi, Tokyo 180, Japan
Phone: +81 422 59 3585
E-Mail: sugawara%ntt-20.ntt.jprelay.cs.net (CSNET)

ABSTRACT

Computer networking is rapidly expanding, and the number of problems occurring in networks is also increasing. Many of these problems have special features which make them difficult to troubleshoot. This paper describes a LAN diagnostic expert system called LODES, which has TCP/IP-related troubleshooting knowledge, and can handle problems occurring in a complex and heterogeneous network environment. Each constituent network has its own expert system containing management information about the local network. TCP/IP-related problems are thus resolved singly or cooperatively depending on their type. This system also includes a network observer which monitors packets flowing in the network and can find a number of problems and problem indicators for automatic problem detection and troubleshooting. This paper describes the configuration of LODES and the knowledge and control methods for cooperative diagnosis, especially the method for cooperative diagnostic task scheduling.

1 Introduction

Computer networks have grown in size and in complexity following rapid advances in internetworking technology. The common internetworking protocol, the Transport Control Protocol/Internet Protocol (TCP/IP) suite, has been implemented in various kinds of computers including supercomputers, minicomputers, workstations, personal computers, and terminal servers. This common use has led to heterogeneous networks. In addition, regional or local networks have been integrated by various media.

The expected diverse network growth has been restricted by ad hoc and problematic network management. Symptoms of problems in local area networks (LAN) include the inability to make a connection between hosts, unintentional disconnection, slow transmission, and network congestion such as ETHERNET meltdown and broadcast storm [1]. However, only a few network experts are able to isolate and resolve such problems. Furthermore, this is very time consuming for several reasons. First, problems that are quite different often have the same symptom. Second, there are sometimes hidden problems, that is, problems that do not exhibit symptoms. Third, the network's intrinsic functions are distributed and its nodes are geographically separated. Last, particularly in a large LAN, each administrator has only local information, which is insufficient for isolating problems.

These problems strongly suggest that a LAN diagnostic expert system is required for automatic, systematic, and effective network management. This system, incorporated into a network, should be capable of finding problems and, if possible, repairing them automatically. Even if problems cannot be eliminated automatically, the system should support human experts by supplying important data automatically collected from the network. It should then store this data for future similar problems.

An important piece of work concerning the TCP/IP diagnostic system is KNOBS/TCP[3]. This system has been investigated as a means of collecting and analyzing packets flowing in the network and for diagnosing problems caused by protocol violations, silly-window syndromes and so on. Its main purpose is to understand the behavior of TCP/IP applications. However, this paper focuses on automatic network management and troubleshooting. Both AT&T and Hewlett Packard Laboratories have built network diagnostic systems [4, 5], but their interests lie mainly in low-level protocol and physical level problems.

This paper describes a diagnostic and observation expert system for a large internetwork. The main features of this system are that it has knowledge related to the TCP/IP-family protocols; it is physically distributed, that is, each network has its own expert system; it diagnoses problems singly or cooperatively, depending on the nature of the problem; and it has a packet observer which automatically detects network problems and problem indications. This system also diagnoses more actively than conventional systems. For example, it not only collects packets, but also sends packets to a host to verify the host's responses. Without cooperative diagnosis, it is impossible to isolate and resolve link-level problems occurring in segments separated by an IP router or gateway, such as problems with communication between hosts in different networks. Of course, packet collection must also be performed in each network. This type of cooperative diagnosis is analogous to a human expert calling a person at...
a remote site to isolate the problem cooperatively.

This paper describes this network management system's architecture, discusses the system's data and knowledge and the roles they play, and represents the communication protocols between expert systems required for distributed cooperative diagnosis. Two performance examples are also described.

2 System Configuration

2.1 Distributed Network Environment

The required diagnostic system must be distributed, since networks offer a physically and functionally distributed environment. The cause of a link-level problem is sometimes located in a remote network. Analysis of packets collected in the remote network gives essential information to the diagnostic system. Two methods for achieving this have been proposed.

1. Each network has a program which collects packets and sends them to a certain centralized diagnostic system.

2. Each network has a diagnostic system which isolates the problem singly or in cooperation with other systems, depending on the nature of the problem.

Although the cost of method (1) is low, it has a number of disadvantages. First, sending many collected packets to another network increases the work load of networks and IP routers. Furthermore, since transmission of IP packets over narrow-band media is very slow, sending collected packets is not an acceptable method in this case. Second, the centralized diagnostic system must know all the IP addresses, routing tables, host information, etc. for diagnosis, but generally centralized management of this data is problematic. Actual network management is distributed to avoid the difficulties of centralized management. Finally, sending packets without encoding to another network is dangerous, because they may contain important data such as passwords. Method (2) is more expensive, but only the results of analysis are sent to another system, reducing the amount of communicated data. The other problems with (1), described above, are also all solved simply. Thus, the required diagnostic expert system must be distributed and cooperative.

2.2 Configuration

The global organization of our LAN diagnostic system is shown in Fig. 1. The system is attached to each constituent network, and a diagnosis can be performed cooperatively by communication between local copies of the expert system when necessary.

The configuration of this system is shown in Fig. 2. The complete system is called the Large Internetwork Observation and Diagnostic Expert System (LODES). The Network OBServer (NOBS) component collects all kinds of packets, and the Network Packet Sender (NePS) component can send any type of packet. Another important duty of NOBS is detecting network problems, problem indicators and abnormal states. The LAN Diagnostic expert system (LAND) component is the main part of this system and contains most of the data/knowledge and diagnostic rules. LAND includes the Remote Network Observer and Sender controller (RNOBS), which controls NOBS and NePS functions such as filtering, triggering, and packet sending, all which are based on diagnostic knowledge. The Communication Handler for Large internetwork Expert Systems (Chales) communicates with the remote LODES for cooperative work. The most important role of Chales is scheduling jobs requested by remote LODES during cooperative work. The arrows in Fig. 2 show

1 A constituent network is a set of segments separated by an IP router or gateway [7]. This expert system ignores bridges, because it is almost impossible to detect the presence of a bridge; hosts do not have information about bridges.
inter-communication paths in LODES. This communication is achieved by using "socket". The socket port numbers are also shown in Fig. 2.

3 The Roles of Data and Knowledge in LODES

3.1 Data and Protocol Knowledge

(1) IP Addresses and Routing Tables
Each LODES must have an IP address table of all hosts attached to its own network and a routing table that shows which IP router can deliver packets to the desired remote network. Each host refers to this table when it starts to communicate with another host.

The routing table is referred to when a host starts to communicate with a remote network host, so it is impossible to isolate a communication problem without it. This data is also employed in communication between LODESs for cooperative diagnosis.

(2) Information Concerning Hosts
Information concerning a host is information about its characteristics. There are two types of information. First is the way the host responds when it receives a packet. Such responses vary depending on the kind of service, the host, and the network software. This information is not essential, but it can reduce the amount of reasoning time. For example, if LAND knows that a host does not look at ICMP echo request packets, then a number of tests, such as sending an echo request packet and waiting for a reply, can be omitted.2

Second is the Media Access Control (MAC) number, which can sometimes specify the machine type. LODES can derive the machine type from this MAC number and also has data on some typical machines.

Information concerning hosts can be automatically collected by sending suitable packets to the hosts during normal network operation. It is not feasible to input this data by hand. The collected data is stored in the Host Information Database.

(2) TCP/IP-related and Upper-Level Protocols
For protocol-related diagnosis, LAND has knowledge on Address Resolution Protocol (ARP), IP, TCP, User Datagram Protocol (UDP), and ICMP. Packets collected by NOBS are passed to LAND and analyzed by this protocol knowledge. These collected packets are usually classified into ARP and IP packets; IP packets are further classified into three groups: for opening connections, for IP data transmission, and for closing connections.

Upper-level protocol knowledge is used when LAND analyzes IP data transmission packets. LAND has typical protocol knowledge such as TELNET, FTP, and SMTP. The representation of protocol knowledge is also an important issue; however, the details will be described in another paper.

(4) Normal Network Status
Knowledge concerning normal network status is required to decide whether the network has a problem. For example, the maximum packet flow rate (byte/sec) in our segment is maximally 250 KB/sec in the normal state. A sudden rise to become 500 KB/sec or more, obviously indicates an abnormal state. Normal network status is measured by statistical data such as collision rate, error packet rate, maximum/average packet flow rate, and maximum/average packet number (packet/sec).

3.2 Diagnostic Knowledge

Since this system is distributed and cooperative, most diagnostic knowledge concerns only a local network and the attached hosts. However, communication knowledge is required for cooperative work between LODESs.

(1) Knowledge for Packet Collection
Appropriate filter and trigger definitions are required to achieve effective packet analysis. It is impractical to analyze the huge number of packets flowing in a segment. Therefore, LAND must send filter and trigger definitions to NOBS to prevent wasteful analysis. LAND has the knowledge to determine appropriate filter and trigger definitions from user reports, the network state and the host state.

(2) Knowledge for Cooperative Work
Knowledge related to cooperative work is required to determine when to initiate the cooperative work, what kinds of jobs are required by the remote LODES, and how and when to respond to a request. There are three means of communication: this knowledge. The first is installation and initialization diagnostic communication (IDC), which sends configuration data to all active LODES for adding a new local LODES system to the network and diagnostic initialization data to some LODES for cooperative diagnostic initialization and negotiation. The second is information delivery and request communication (IDRC), which is for sending/requesting important findings to/from remote LODES. Diagnostic Control Communication (DCC) can control remote LODES activities such as synchronous packet collection and stopping or interrupting the diagnostic process.

(3) Diagnostic Knowledge about the Local Network
This knowledge is comprised of information for isolating a problem whose cause is in the local network. An example of simple diagnostic knowledge written according to a production rule is shown in Fig. 3. Diagnostic knowledge is divided into control knowledge described in production rule formulae, and investigation knowledge written in production rule formulae, LISP, and C (Fig. 4). Control knowledge and investigation knowledge are interpreted by their respective interpreters. Both kinds of knowledge can access a shared memory area called a blackboard [2]. When accessing it, control knowledge selects one item to be investigated in the next cycle. The chosen item is investigated by applying investigation knowledge, and the result is stored on the blackboard.
If No ICMP echo reply is found in *H
*H is attached to another network *N
Then Check *H by LODES *L
*L manages *N
Set the status number -1

If Multiple ARP replies are observed
Then Get their sender's MAC numbers
Check if one of them is new

Fig. 3 Example of Diagnostic (Local Plan) Rules

Control Knowledge Interpreter refer

Investigation Knowledge Interpreter refer

Control Knowledge (production rules)
Investigation Knowledge (production rules, LISP and C programs)

Fig. 4 Diagnostic Knowledge Classification and Diagnostic Cycle

Then a new item is chosen and the cycle is repeated until the
cause is found. This cycle is called the diagnostic cycle. The
items chosen by control knowledge interpreter are called ac-
tive investigation items or simply active items in this paper.

A blackboard3 in this system briefly described in Fig.
5. It consists of several item name and item value pairs. An
investigation job investigates an item and adds the result to
the blackboard. The result of this job is called an item
value in this paper.

ITEM 1: ITEM VALUE 1
ITEM 2: ITEM VALUE 2
ITEM 3: ITEM VALUE 3
.......

Fig. 5 Blackboard Structure

3.3 Knowledge for Observation

The network must be monitored to detect problems or prob-
lem indicators so they can be resolved as early as possible.
To detect network congestion and network load, errors, the
network load, collision rate, and error packet rate are mea-
sured statistically and compared with those of a normal net-
work. This method can detect a number of problems such as
ETHERNET meltdown, broadcast storm, ACKing ACK,
and bad contact with a transceiver (cable).

NOBS also detects the following packets, which may some-
times be the cause of network congestion.

- BOOTP (UDP)
- RIP or ROUTED (UDP)
- RWHO (UDP)
- RARP
- TFTP (UDP)
- ICMP mask request (broadcast)
- ICMP unreachable

The selection of these packets was based on our networking
experience. Other examples of important conditions for
monitoring are as follows:

- Multiple (proxy) ARP replies
- ICMP time exceeded packet
- Wrong IP broadcast address
- Packet whose sender's MAC number is broadcast
- Packet sent from an unauthorized host
- Unauthorized protocol packet

After detecting one of these packets or an abnormal net-
work state, NOBS sends this data to LAND and/or warns
network managers of it.

The knowledge described in this subsection is contained
in NOBS. It is written in the C language to improve perfor-
mance and make real-time analysis practical. Note that the
important point in packet monitoring is not to avoid network
problems, but to make timely packet collection possible.

4 Diagnostic Method

The diagnostic process is started by a complaint from a user
or a report from NOBS. Because users can only detect per-
ceivable phenomena, the types of symptoms they report are
restricted to only a few. Users usually report one of the
following:

(1) Connection cannot be established with a host.
(2) Transmission rate is low (slow transmission).
(3) Connection is unstable (connection sometimes resets,
communication is sometimes disconnect, or transmis-
sion rate is erratic).

In the diagnostic process, the reported or detected prob-
lems are classified as either local or non-local problems. A
local problem is an individual network problem whose cause
is in the local network. A single LODES resolves these prob-
lems. A non-local problem is one whose cause is possibly in a
remote network. This type of problem is resolved through co-
operation between multiple distributed LODESs. Note that
LODESs cannot always immediately determine which kind
of trouble is currently causing the abnormal state. This is
determined during diagnosis.

Diagnosis is usually performed by analyzing a combina-
tion of the following:

1. Packets collected in the network (on all protocol levels)
2. Statistical measurements of the network, such as network load and collision rate.
3. Reply packets to a test packet transmitted to a host.
4. Routing information in IP routers (using SNMP).

Packet collection at multiple points and test packet transmission from a remote LODES are important for diagnostic analysis in cooperative diagnosis. The result of test packet transmission is compared with the result of test packet transmission by the local LODES. The difference in these results also offers significant data for determining the host state.

Detailed discussion of the diagnostic method is beyond the scope of this paper. Communication and methods for cooperative work are discussed in the next section.

5 Communication between Expert Systems

5.1 Configuration
Each LODES has data called LODES route data, as shown in Fig. 6, for communication with remote LODES during cooperative diagnosis. When a new LODES is attached to a network and there are changes such as modifications to a LODES IP address or a management network address, installation protocol, which is a type of IIC, causes the LODES route data to be updated. Route data is built and maintained using Simple Network Management Protocol (SNMP) [8, 9, 10], but currently this feature is not implemented.

5.2 Initialization and Diagnostic Arrangements
The purposes of the following four types of communications are to arrange and negotiate the start of cooperative troubleshooting.

(1) Connection verification
(2) LODES state request
(3) Route exploration
(4) Diagnostic arrangement

These are all forms of IIC. Communication (1) verifies that connection can be established between a local LODES and a remote LODES. A remote LODES state, such as 'BUSY' or 'WAIT,' is required to start cooperative diagnosis. This is realized by (2). If (1) fails, that is, connection cannot be established, (3) explores the route to the remote LODES and investigates discrepancies in the LODES route data and their causes. Currently, this exploration is not implemented. However, it will be implemented using SNMP in the future. Communication (4) is required to make arrangements with intermediary LODES systems which manage the constituent networks on the way to the remote host.

5.3 Diagnostic Communications
Diagnostic communications, which belong to IDRC or DCC, are used when a LODES needs to control a remote LODES, obtain data from it, or send data to it. For example, a request for a remote host table, routing table, remote host information, statistical measurements of the remote network, delivery of the diagnosis result, and synchronous packet collection are performed by these communications. They belong to IDRC or DCC.

We can see that a diagnostic communication by IDRC is a request-to-investigate job, because these communications obtain item values and put new values on the local blackboard. Any request by IIC, IDRC, or DCC is called an R-job.

5.4 Responses to Requests from Remote Systems
From the viewpoint of side-effects to the diagnostic process and strategy in the local LODES, R-jobs from a remote LODES may be classified into non-side-effect R-jobs, side-effect R-jobs, and synchronous R-jobs (see Fig. 7). The following are examples.

- Non-side-effect R-job: R-jobs requested by IIC and requests for items which have already been investigated by the local diagnostic process.
- Side-effect R-job: DCC, delivery of a new result from the remote LODES, and requests for items which have
not yet been investigated by the local diagnostic process.

- Synchronous R-job: Synchronous packet collection and packet analysis.

A LODES sending an R-job request packet is called a client, and a LODES receiving it is called a server.

Chales can respond to a non-side-effect R-job independent of a LAND process, because the blackboard, which is memory area shared by LAND and Chales, is the only means by which Chales can reply. Any synchronous R-job in this system is a time-consuming job, because it must be synchronized by all LODESs working cooperatively. Thus, an R-job is controlled and scheduled as follows:

1. Investigation items are divided into two groups, synchronous and asynchronous, which can be determined a priori, and can be investigated by synchronous and asynchronous R-jobs (see Fig. 7).

2. First, each LAND investigates as many asynchronous items as reasonably possible. Based on the results, a number of synchronous items are executed. The asynchronous items are then checked again, and this cycle is continued until the cause is found. Thus, a synchronous R-job starts only when LODES cannot find the cause without it.

3. For synchronous R-jobs, the local LODES, which has received a user report or a problem detection from NOBS, synchronizes all working LODESs.

Requested side-effect R-jobs are divided into four groups called the standings: preferential, ordinary, postponed and rejected. R-jobs from other LODESs are scheduled once in a diagnostic cycle and selected as follows:

- If preferential R-jobs are requested, LODES responds to them.
- If ordinary R-jobs are requested, one is selected and its results are returned to the requesting LODES.
- Postponed R-jobs are performed while the LODES is waiting for a synchronous R-job or when the LODES's own diagnosis is completed.
- A rejected R-job is ignored.

This classification of R-jobs is carried out according to the status numbers shown in Table 1.

<table>
<thead>
<tr>
<th>Number</th>
<th>Diagnostic Status of LODES</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 (urgent)</td>
<td>Set by a system administrator to stop the diagnostic processes.</td>
</tr>
<tr>
<td>2</td>
<td>LODES concludes that the cause is in its management network.</td>
</tr>
<tr>
<td>1</td>
<td>LODES infers that the cause is possibly in its management network.</td>
</tr>
<tr>
<td>0</td>
<td>No information or initial state</td>
</tr>
<tr>
<td>-1</td>
<td>LODES infers that the cause is possibly in another network.</td>
</tr>
<tr>
<td>-2</td>
<td>LODES concludes that the cause is in another network.</td>
</tr>
</tbody>
</table>

R-job standing of the requested side-effect R-job.

The remaining issue is how to determine R-job types. We can know a priori whether an R-job is synchronous or asynchronous from the facts contained in the control knowledge and investigation knowledge. In contrast, it is impossible to distinguish between non-side-effect R-jobs and side-effect R-jobs a priori. If the server already knows the item value, the R-job is non-side-effect; otherwise, it is side-effect. This is because the diagnostic process and the strategy are sometimes affected by new facts. Thus, the server decides the type when an R-job is requested. DCC is always side-effect. Note that the R-job types may vary depending on the progress of the diagnostic process or the status number.

6 Examples

6.1 Cooperative Troubleshooting

Suppose that the system administrator using this expert system receives the following complaint.

```
I logged onto host P, then tried to log onto host Q from P using TELNET, but the connection could not be established. Host Q is attached to a remote network (so its path from P to Q has a number of IP routers).
```

In this case, the possible causes are: P or Q has a problem, an IP router is not functioning, one of the networks to Q is busy, and so on. The Fig. 8 is the actual trace of the main diagnostic processes using the local and remote LODESs. The cause of the problem is an incorrect routing table in host Q. At 3, LODES suspects that its own network and host P do not have a problem, and at 4, IP routers along the way have no routing problems. Items 4 and 5 are communicated by IIC. At 6, LODES checks whether Q always sees an ICMP echo request packet when looking at the Host Information Database, and the answer is yes. The R-job request in 10 is a request that the local LODES sends an ICMP echo request packet to Q. At 14, LODES is aware that host Q has a problem; two probable causes are the routing definition in host Q is wrong, or the wrong network interface hardware name is assigned in Q.

During remote LODES operation, the local LODES also
4.3 performed, for example, the local LODES looks into host P.

While 6 - 10 are being performed, for example, the local LODES looks into host P.

Two possible causes are: P has an incorrect routing table, or if P is a SUN machine, it may be in single-user mode or INETD may not be working.

Note that, in this case, the routing table in Q can be corrected by sending an ICMP redirect packet to LODES, but this sometimes causes another problem: host Q may be intentionally hidden from another network. Thus LODES sends a redirect packet only to hosts which are allowed to receive it.

6.2 Autonomous Work

The packet data in Fig. 9 is collected by NOBS and it shows that there are two ARP replies. This kind of data is sent to LAND and is diagnosed automatically.

IP addresses and MAC numbers are checked in LAND to determine whether they are proxy ARP replies and which MAC number is correct based on the MAC number database in LODES. If they are proxy ARP replies, LAND recommends to the network manager that only one of the IP routers should reply to proxy ARP. If an incorrect MAC number is seen, LAND checks the internal table to determine whether its host has been changed.

6.3 Performance

In the first of the above examples, elapsed time is about 46 seconds, and run time is approximately 7.85 seconds in total. Almost all run time is used for analyzing collected packets. The difference between run time and elapsed time is the waiting time for the reply packets. In the second example, elapsed time is about 15 seconds, and run time is about 8 seconds. Almost all run time in this case is also used for analyzing collected packets. Note that run time does not include garbage collection in LISP.

Comparison of the performance of this expert system with that of a human expert is difficult; a human expert can resolve problems that are more complex and difficult, but this expert system is not designed as an all-round troubleshooter. However, if the expert system can find the cause, it is much faster than a human expert. It is almost impossible even for a human network expert to resolve problems such as the above examples within one or two minutes. Furthermore, because this system can resolve frequently occurring problems, it can prevent wasting a human expert's time. Moreover, some abilities of the Network Observer are beyond human ability, (e.g., a human cannot monitor packets continuously).

LODES can find the cause of almost all protocol problems except those concerning layer one. Problems caused by incorrect host configuration can also be diagnosed, but OS and communication software information is required. LODES has such information for BSD4.3 and UNIX System V, so if the host is one of these types, it can diagnose the host problems. It should also be noted that some layer 1 problems, such as network short circuits and a bad connection transceiver, are detected by LODES by observing packet flow information. Important data for detecting these problems are the volume of packet flow and the packet error rate.

6.4 Implementation

This system is implemented in COMMON LISP (Kyoto Com-

TCP nwturn.telnet > tip-1.62847 ...PA. L:1 S:55447674 A:1306460763 W:4096
TCP tip-1.64505 > ntt-20.telnet ...IPA. L:1 S:1307336283 A:-1036775238 W:1519
TCP gulis.telnet > ntt-20.33729 ...PA. L:1 S:1211245137 A:-1023803300 W:2048
ARP 6:0:2b:6:46:52 ff:ff:ff:ff:ff:ff mtgosoo looks for the ether address of lucifer
TCP ntt-20.telnet > tip-1.64505 ...PA. L:1 S:-1307336283 A:1306775238 W:1330
ARP 8:0:20:0:7:76 8:0:2b:6:46:52 lucifer replies to mtgosoo its ether address is 8:0:20:0:7:76
ARP 8:0:46:0:1d:dc 8:0:2b:6:46:52 lucifer replies to mtgosoo its ether address is 8:0:46:0:1d:dc

Fig. 9 Collected Packet Output Example

This data format is designed along the lines of Van Jacobson's tcpdump program, but output from NOBS is more flexible.

\footnote{This data format is designed along the lines of Van Jacobson's tcpdump program, but output from NOBS is more flexible.}

\footnote{UNIX is a trademark of AT&T Bell Laboratories}
mon LISP) / SUN3 (SUN OS 3.5) and C. NOBS, RN0BS, NePS and Chales are written in C, and LAND are done in LISP. The knowledge representation and reasoning methods are implemented by KNAC, which is based on KRINE [6] expanded by a number of added functions for cooperative work. KNAC is not described here. Knowledge in LAND is mainly represented as production rules and a PROLOG-like language, although some investigation knowledge is described in LISP or C.

7 Summary

The cooperative local area network diagnostic and observation expert system described in this paper has the following features: each constituent network has a copy of the diagnostic system; cooperative troubleshooting of TCP, UDP/IP-related problems and their upper-level protocol-related problems is supported; some problem detection by the Network Observer is automatic. The configuration of this system, the knowledge contained in it, and its cooperative diagnostic methods were described. Introduction of this system in networks should allow quick resolution of various problems and facilitate network management.

As an artificial intelligence application, this system has the interesting feature of distributed and cooperative diagnosis. In the first phase of this system's development, we thought that it should not be used for distributed diagnosis, because this usually requires difficult and complex tasks. It was thought that the difficulty of such task would outweigh any benefits. However, during development, we realized that the system should be distributed and that it could be implemented for cooperative diagnosis. This configuration is more natural in terms of network structures and management. Having come to this conclusion, the main issue, became communication methods, job scheduling, and control.

From another viewpoint, LODES consists of two expert systems: NOBS, which is a network observation expert system, and LAND, which is a network diagnostic expert system. Communication between NOBS and LAND is communication between two different expert systems, which is the second interesting feature of this system. Currently, research into coordination of different kinds of expert systems is becoming more important to progress in networking, distributed systems, and distributed software environments.

Detailed discussions on NOBS, RN0BS, NePS, and lower-level structures such as the packet header format and methods of diagnostic communication are not dealt with in this paper. These topics are discussed elsewhere [11, 12].

Acknowledgment

I wish to thank my colleague, Ken-ichiro Murakami, for his helpful comments and advice. Almost all of the knowledge contained in this system is derived from his experience. I would also like to thank Shigeki Goto for his constructive comments and for supplying the motivation to develop this kind of network diagnostic expert system.

References