Network Fault Diagnosis: a Model Based Approach

J. Wainer
IC - UNICAMP
Brazil
wainer@dcc.unicamp.br

L. Barros
IME - USP
Brazil
leliane@ime.usp.br

V. Bernal, M. Lemos
LSI - USP
Brazil
{*volnys,mlemos*}*@lsi.usp.br*

Most of the diagnostic systems for computer network faults discussed in the literature or available as part of network management platforms are experience-based systems. Such systems, in some way capture the experience of detecting a fault on a particular computer network.

A subproblem of fault diagnosis, the alarm correlation problem, that is, the filtering out irrelevant, or explained, or spurious alarms once a fault is detected have been approached by other experience-based methods. For example, neural networks that learn from previous experiences of the same network, which alarms are expected to follow some particular alarm, and may filter those "expected" alarms. The problem with experience based systems is that they only work for that particular network. If a particular network is changed, it is very likely that a case based systems, or a neural net learning system , and any other experience based system will be useless.

This paper presents a model-based approach to fault diagnosis in computer networks. The idea behind a model based diagnosis is to have a complete description of the local area network: the topology, type of equipments, routing tables, and so on. With this information and the knowledge of how IP packages travel in the network, one is able to perform a model based reasoning for this network.

In order to construct the complete model of the network we developed a module that discovers the network model automatically. Thus, if the network is changed, this network discovery system will automatically (or semi-automatically) reconstruct the complete network model for the new configuration.

The diagnostic system is composed of different subsystems, which run at different moments. The off-line subsystem has two components, the Network Discovery System (NDS) and the Configuration Diagnostic System (CDS). These two systems generate and criticizes the network model.

The online subsystem has two components, the Network Status Gathering System (NSGS), which collects information about communication faults from the network, and the Communication Fault Diagnostic System (CFDS), the central component of the system, which receives the information of some communication fault, and interacts with the network model, to discover a set of diagnostic hypothesis. Each diagnostic hypothesis is a list of network elements and connections, and to the best of the system information at least one of these elements and connections is faulty.

NDS. We have developed a NDS that collects information about the subnetwork structure, the equipment identification, and most important, connections among the equipment. The NDS makes uses of the following: SNMP ARP table from MIB-II [RFC1213], SNMP route table from MIB-II [RFC1213], Bridge MIB [RFC1493] and Repeater MIB [RFC1516].

CDS. Because the fault diagnostic system need a consistent and complete network model, it was necessary to implement a system to analyze the discovered network model. Therefore, the CDS interacts with network model in order to find out possible configuration errors. Only when no errors are found the network model will it become available to the fault diagnosis system. We discovered that in a moderately large network, of hundreds of network element, there was around a dozen configuration problems, from network elements with no name, to inconsistent routing tables.

NSGS. The NSGS is the component that queries the network to determine its status. In the case of this work, we are only interested in communication faults, so the only information collected by the NSGS is whether a network element is reachable or unreachable. This is done by cyclicly pooling the network elements.

The relation between the diagnostic system and the NSGS defines different classes of diagnosis. An Active diagnostic system obtains network information by requesting data from the network environment. This type of system has a high degree of autonomy, being able to decide and to request additional information from network environment during the diagnosis process. A Passive diagnostic system waits for the information to come from the NSGS, e.g., it does not make any information request. Typically, a NSGS gathers information about the network objects through a pooling cycle and makes that information available to the diagnostic system.

Some management platforms gather information about the network objects, but does not make them available. Only transitions from normal to faulty states, and back, are made available to other systems. From the diagnostic system's point of view, the passive by transition mode is somewhat more complex, since information about the status of network elements is provided only once.

We developed three algorithms for the three modes of diagnosis. The active mode algorithm assumes that there is only a single fault, which is reasonable since once evidence is found that there is a fault, it quickly discovers the source. The algorithms for the other modes only assume that the number of faults is minimal, that is one cannot remove any of the proposed faults and still explain all the abnormal observations.

The NDS was implemented on top of the ISM Open Master (Integrated Management System from Bull Company) management platform. It was tested in a large local area network with hundreds of heterogeneous network elements. The CDS was implemented in Prolog, and tested with the data generated by the NDS on the large LAN. The three diagnostics algorithms were implemented in Prolog, and tested in an artificial environment (artificial network model and simulated events from the NSGS). The passive by transition algorithm was integrated with the Open Master NSGS in a small network, for which the NDS could discover a complete network model. This work was funded by ABC Bull SA Telematic.