Workshop Note: Artificial Intelligence for Fault Management Problems

Beat Liver*and Sue Abu-Hakima†

May 18, 1999

Abstract

With rapidly updating network technology and increasingly heterogeneous deployed systems, network fault management remains one of the foremost network management challenges. Work in the past has shown that Artificial Intelligence techniques have considerable potential in the area. This paper describes a generic fault management problem with the aim of stimulating discussion at the AiDIN'99 workshop held at AAAI'99 in Orlando, Florida.

1 A Generic Problem Description

Perhaps the easiest way to understand the issues in a domain is to relate them to a generic problem definition. The following fault management problem will hopefully provoke discussion at the AiDIN workshop. The specification is divided up into three parts: Section 1.1 for the problem definition, Section 1.2 gives an example configuration to illustrate the problem and Section 1.3 gives a brief description.

1.1 Definition

A Connectivity Provider (CP) provides a connection-oriented broadband service (e.g., ATM), which is used by; an IP Provider (IP) and a Corporate Network (CN). The Corporate Network consists of IP-based Local Area Networks (LANs) at several different sites. These CN sites are sources of IP traffic.

The connectivity provider may operate various types of technology and topology setups. The IP Provider operates backbone routers, each of which is attached to a (co-located) CP node that also provides an ATM connection

*IBM Research Division, Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Rueschlikon, Switzerland. e-mail: (bli@zurich.ibm.com)

†AmikaNow! Corporation, Industrial Partnership Facility, Building M-50, Montreal Road, Ottawa, Canada, e-mail: (suhayya@amikanow.com)

to the CN site. It is sufficient to consider only switches and routers as network elements, although the network may also contain other network management entities and computers (i.e., servers, personal computers etc.).

Each network node correlates the events it observes locally, based on which each network (i.e., that of the service provider and that of the corporation) presents a global and integrated view at a central management station. This means that a network provides an abstract view of itself to its clients (i.e., CN is a client of IP, which is a client of CP). It is assumed that clients obtain events with respect to their subscribed services.

1.2 Example Configuration

The following is an example configuration for this type of network scenario (To help illustrate the problem - it may also be used as a reference to aid comparison):

- There are 3 CN IP LANs at three different sites.
- The Connectivity Provider operates a ring-topology ATM network (with 6 nodes), in which the traffic flows clock-wise and counter-clock wise.
- This network offers protection switching, i.e., in case of a node or link failure, the traffic is rerouted within 400ms (unless the detection mechanism fails).
- It can be assumed that there is enough capacity in the ring network during all fault free operation.
- The IP Provider operates 3 backbone routers which interconnect three CN routers (located at different sites). Each router interface monitors its associated lines and reports line failures after 200ms (during which no traffic flows on the line).
- The IP provider offers a priority and best-effort service. The customers of the former are guaranteed to have connectivity (under a single line failure assumption), whereas the best-effort service may not be available.
- The IP Provider's backbone network is operated at an average line load of 80%, where 50% is priority traffic and 30% best-effort traffic on each line.

1.3 Description

In the resulting layered network, a component either works, does not work or works incorrectly. The task is therefore to take the network setup and to detect, diagnose and deal with failure events. These should then be presented at the

central management stations of the various networks. To facilitate comparison, authors are encouraged to focus on the identification of the working/not-working subcomponents and the consequences on the state of components and the whole system. Example events for the specific instance of the scenario given above are:

- An interface card fails to detect that the line attached to it is broken.
- Physical lines of the CP ring-network and the access network are be broken.