Chapter 11. Introduction to Network Management 1

Table of Contents

Introduction to Network Management 1

Context

Networks of all the types that have been dealt with so far in this module need to be managed if they are to operate efficiently. In this way, this unit relates to all the previous units. In addition, network management is needed to ensure that networked applications such as e-mail and market places make best use of the networks over which they operate, which relates this unit to many of the following units. Finally, many of the techniques of network management are needed in the construction of Distributed Systems which are treated in general terms in chapters13 and 14.

Introduction

A general account of the overall architecture of a network management system is described. Network monitoring, the collection of information on the status of the network, the consolidation and interpretation of this information, and acting on the resulting interpretation are distinguished as the major activities of a network management system. The way in which these activities are realised, the co-ordination of the activities, and their embedding in one coherent network management system are all treated. Various examples are given of the type of network problem that a network management system is responsible for. The way in which a generic management system deals with these problems is then illustrated.

The generally accepted classification of network management activities into five broad problem areas, that is, fault management, performance management, configuration management, accounting management and security management, is presented.

The idea of an 'alert' is then introduced, and it is then shown how generic problem management spanning all these categories may be achieved both manually and automatically on the basis of a process that is driven by the use of alerts.

Objectives

At the end of this module, you should be able to:

- rehearse the concepts and concerns of network management;
- classify network management activities;
- provide examples of network management activity;
- outline the principles underlying the implementation of network management systems.

What is network management?

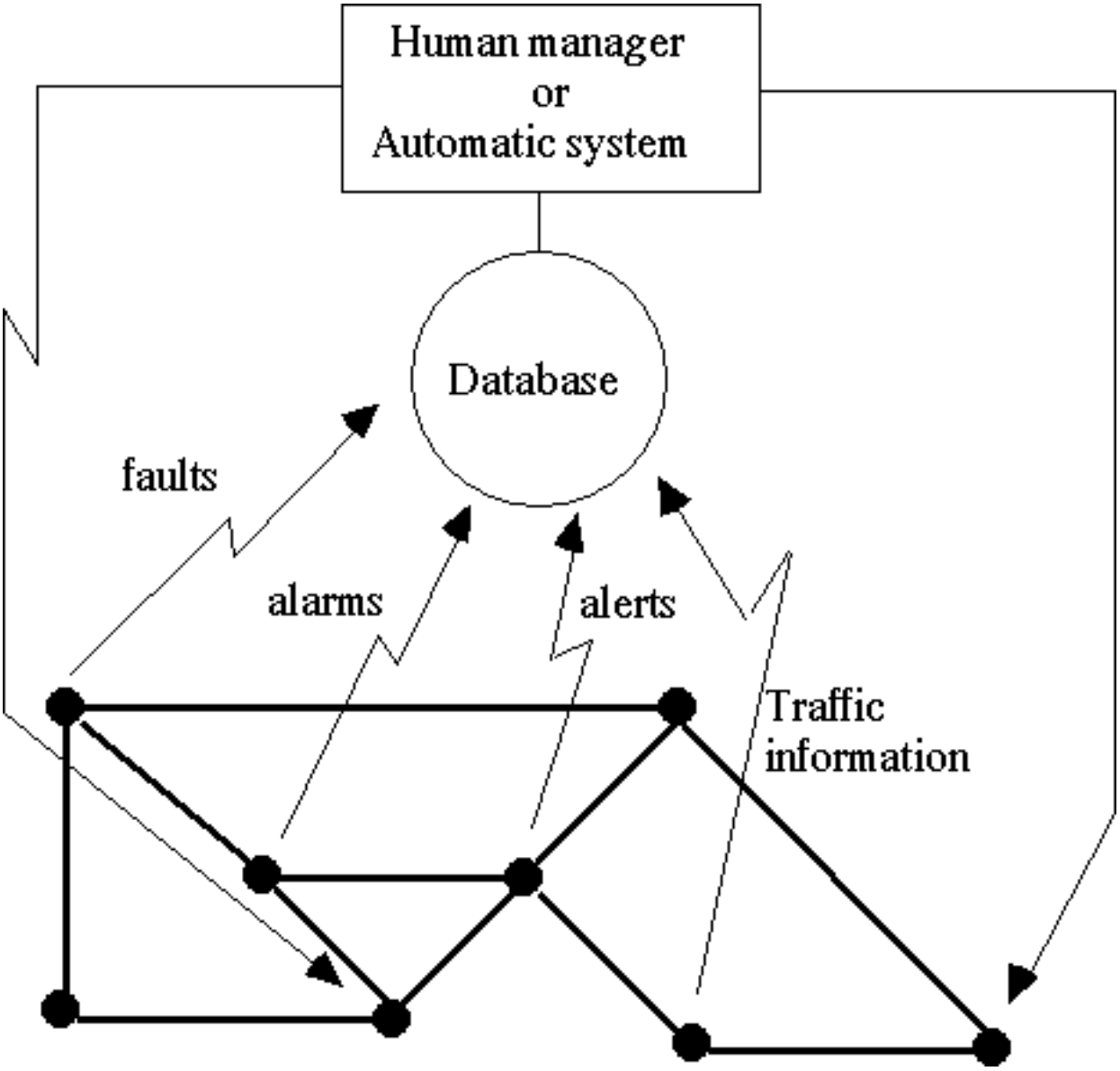
In parallel with this topic, you should read Chapter 19 of W Stallings, "Data and Computer Communications", (6th edn.), (Prentice Hall)

When a network is seen as a single entity, that is, as one collection of resources, two views of network management can be offered.

The first construes network management as the monitoring of the activities of a network, following which the information collected is consolidated to present an overview of the state of the network to a human operator who can then take any actions necessary to improve the operation and performance of the network.

The second view understands network management as a completely automated process in which a network is monitored, and the information obtained is consolidated and then presented to an entity capable of automatically determining from it the actions necessary to adjust and adapt the network so that it maintains the required levels of operation and performance.

These views can be illustrated as follows:



To Do

Do Review Questions 1, 2 and 3.

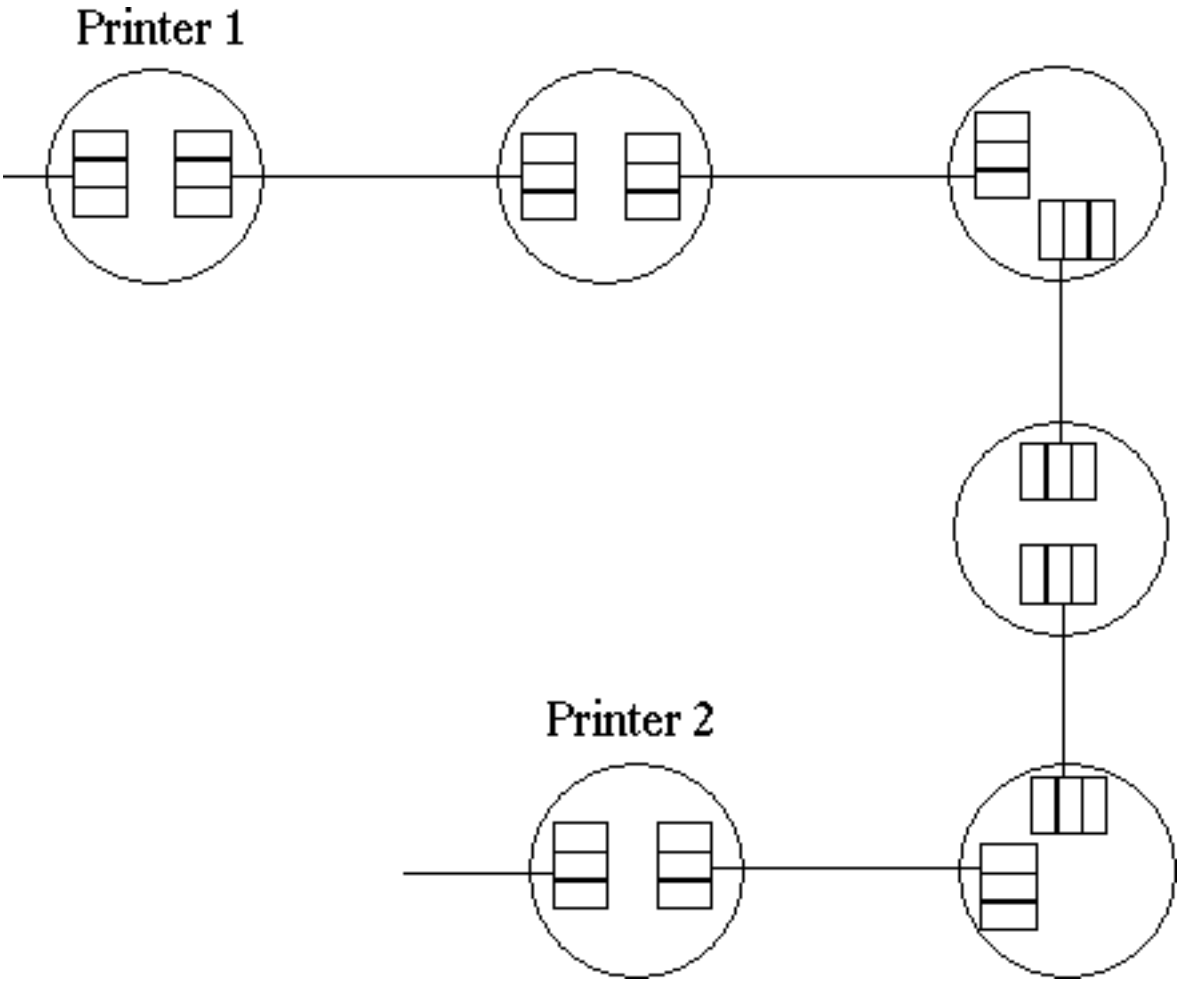
Examples of network management activity

The following list give some examples of activities that are typical of those undertaken by a network management system.

1. Monitoring the computers and links of a network to detect any faults that may develop in them.

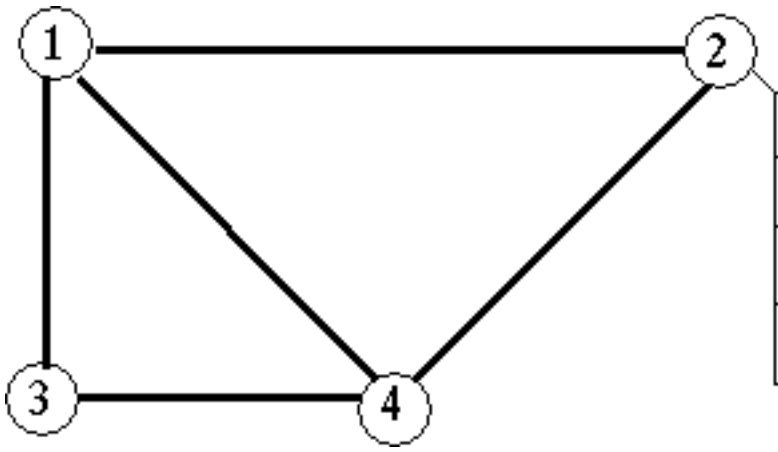
2. Monitoring the message queues at each computer to ensure efficient use of network resources and prevent message loss.

   The illustrated network segment contains two printers. When one of them is busy, which is apparent when its queue of waiting jobs becomes full, computers with a job to be printed will be directed to send it to the other printer.



3. Controlling the routing of messages through the network. This is a way of routing round a fault detected by the monitoring of example 1. It also provides a way of avoiding the busy parts of a network where a message would be delayed.

   When computer 4 is busy, the routing table at computer 2 can be changed to route messages for computer 3 via computer 1.



dest.	send to
1	1
3	4
4	4

To Do

Do Review Questions 4, 5 and 6.

Classification of network management activities

We have touched on some network management activities in the previous section. There is a generally agreed classification of all the activities that assigns them to one of the following problem areas:

Fault management: The concerns of fault management are the detection of faults, and covering up for them until they can be repaired, after which the network can be returned to its original state. Faults can be covered up by working around them or by providing some alternative that is functionally equivalent to the failed unit.

Configuration management: The configuration of the network is the arrangement of its computers and links, that is, its topology. Configuration management deals with changes to the configuration of the network caused by the addition and removal of computers and links.

Performance management: Managing the performance of a network involves maintaining an acceptable quality of service for all its users. This usually involves the delivery of messages within some specified time. Occasionally, acceptable levels of service may be expressed in terms of levels of reliability. Acceptable delivery times can be achieved by managing the flows of traffic across the network and, as far as possible, preventing the build-up of congestion. Reliability can be ensured by invoking the necessary measures against message impairment and loss.

Accounting management: The responsibilities of accounting management are to keep track of network usage and, correspondingly, to generate bills for the users of the network.

Security management: The concern of security management is to ensure security both for the network itself and for the users of the network. The security of the network can be ensured by allowing access only to authorized users, and by ensuring that those with access do not use it improperly. The users of the network can be given

the levels of security they need by providing the appropriate security services.

To Do

Do Review Questions 7, 8 and 9.

Problem management

The types of problem management listed above can be managed by adopting the following procedure:

1. Determine that there is a problem. Much of the network monitoring activity is intended to determine whether network components are operating correctly. Components can send an alert if they detect a problem in their own functioning.

2. Diagnose the problem. Find out exactly what the problem is either directly if it is possible or by collecting evidence and deducing what the problem is.

3. By-pass the problem. Work round the problem to ensure that the rest of the network is not affected by it.

4. Resolve the problem. Fix the problem, and then return the network to its original state.

5. Keep a record. Store an account of the problem, so that there is a record. The complete log of problems may well contain valuable information about the running of the network, revealing the presence of persistent problems, recording ways of handling problems, and so on.

To Do

Do Review Question 10.

Carry out Activities 1, 2, 3 and 4.

Implementing problem management

The problems in a network can be determined in two basic styles. The network can be actively monitored by making regular observations of all its components, or the components of the network can send a report when they detect a problem either in their own working or in the working of another component. Given the size and complexity of many networks, it is not surprising that the latter approach is the more common.

Problem management, then, is often done with the use of 'alerts'. An alert is an unsolicited message generated within the network, and sent to the Network Management Centre to alert it to something needing its attention. An alert usually takes the following form:

Typical alerts could take the form:

alert, computer_1, line-6

(Computer 1 complaining about one of its links.)

alert, computer_25, neighbouring_computer

(Computer 25 complaining about a neighbouring computer.)

Note that alerts will usually arrive at the Network Management Centre in clusters. In the first example above, line_6 has computer_1 at one end, but it will have another computer at the other end and, if the line really is faulty, the other line will detect it and will also send an alert sooner or later. In the

second example, the faulty neighbour of computer_25 will also cause a cluster of alerts to be sent in due course.

To Do

Do Review Questions 11 and 12.

Automatic network management

One way of carrying out network management automatically is to use an expert system that has knowledge both of the network under management and of ways of managing it. A simplified version of just such an expert system is presented here. The presented system is intended to manage any faults that may develop on the links of a network. Its stylised form of knowledge representation is based on the use of relations between entities and is much the same as that used by Prolog.

The network under management is shown below. We first consider the automatic management of faults occurring on the lines of the network. Each line can be in one of the three states:

1. in-service,

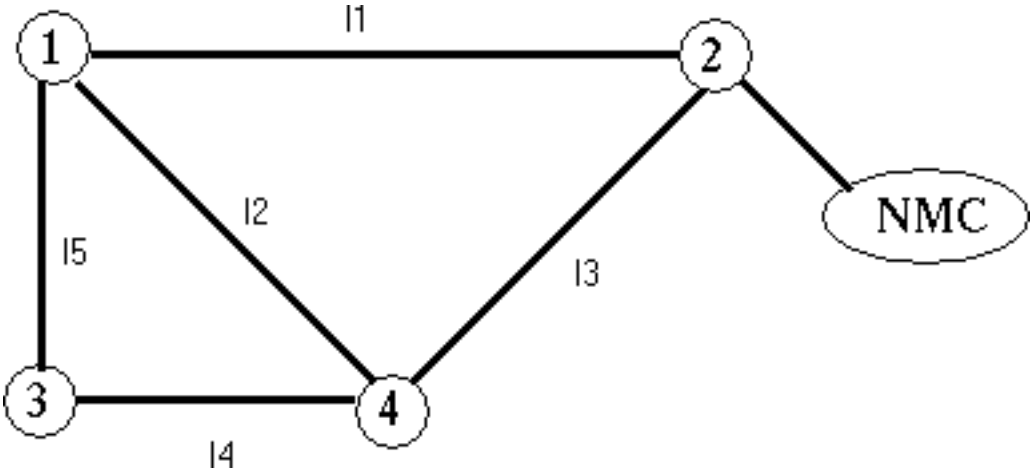
2. out-of-service

3. in-test.

A computer can send an alert about one of its incoming lines. The alert takes the form:

alert, C, L

which indicates an alert from computer C concerning line L. All alerts are sent to the Network Management Centre (NMC), and this is where the expert system is located.



The management expert system contains knowledge about the configuration of the network under management. It is represented as follows:

c1 is-start-of l1
c2 is-end-of l1
c1 is-start-of l2
c4 is-end-of l2
. . .

Knowledge about the state of the network must be represented. Initially it is :

in-service is-state-of
in-service is-state-of l2
. . .

The knowledge for handling faults on the lines is:

IF in-service is-state-of L
AND alert, C, L
THEN in-test is-state-of L
IF in-test is-state-of L
AND ok is-test-result-for L
THEN in-service is-state-of L
IF in-test is-state-of L
AND not-ok is-test-result-for L
THEN out-of-service is-state-of L
IF out-of-service is-state-of L
AND ok is-test-result-for L
THEN in-service is-state-of L

Other problems, notably faults with computers of the network, can be managed in similar fashion as long as the management system has the necessary knowledge about the state of the network, to be able to identify problems, and about problem management, to be able to manage them.

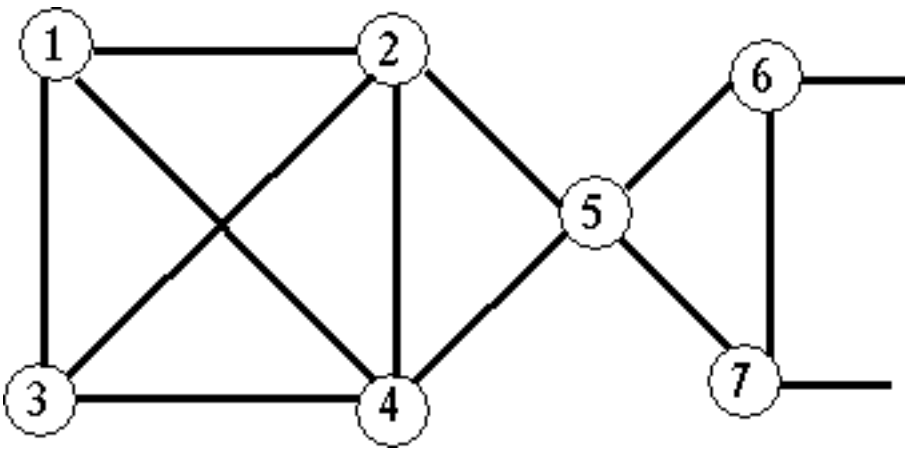
To Do

Carry out Activities 5 and 6.

Network management: an illustrative example

This section aims to present a simple network management scenario that brings together what we have learnt so far.

Part of a network that is under management is shown in the diagram.



The basis of its management is the use of alerts, which are sent to the Network Management Centre (NMC) and take the form:

alert, <sending_computer>, <symptom>

These alerts do not pinpoint the precise nature of the problem, as those used in the previous section did, but provide a symptom or an indication of the problem. The Network Management Centre must diagnose the actual problem by making deductions from the information provide by a cluster of alerts.

There are two matters of concern that are to be managed on this network. One is described here, and the other in Activity 7.

The matter that concerns us here is that a certain number of errors inevitably occur on the links of a network. An increase in the error rate of a link is often a sign that the link is about to fail. For this reason nodes often monitor the error rates on their incoming links. On this network, if the error rate on a link reaches a dangerously high level, any computer attached to that link is required to send an alert. When the sending computer is computer_3, the alert takes the form:

alert, computer_3, high_error_rate

Stage 1 The alert arrives, indicating that some problem exists.

Suppose it is the alert given above. But we know that alerts arrive in clusters and, assuming that it is the line between computer_3 and computer_2 that is causing the problem, the next alert to arrive will be:

alert, computer_2, high_error_rate

Stage 2 This stage is now reached. From the cluster of two alerts, the NMC can deduce that the link between computer_3 and computer_2 may be about to fail.

Stage 3 The management system must now work around this link and also send a technician to fix or replace the link.

Stage 4 When the link has been repaired, the management system can restore the network to its original state.

Stage 5 An account of the problem and the problem management activity is recorded in the log.

To Do

Carry out Activity 7.

Activities>

Activity 1 - problem managers

The problem management procedure described here is, in fact, a familiar procedure carried out by 'problem managers' we encounter in our everyday lives. It is in no way specific to network management. Identify some every day 'problem managers' who follow this procedure.

You can find a discussion of this activity at the end of the chapter.

Activity 2 - problem log

Investigate the kinds of information that could be mined from a network's problem log.

You can find a discussion of this activity at the end of the chapter.

Activity 3 - routing tables

When a performance management strategy of spreading traffic evenly across the network is adopted, the routing tables need to be continually changed to adapt to the state of the traffic in the network.

Describe how the information that is needed to determine the appropriate changes to the routing tables may be obtained.

You can find a discussion of this activity at the end of the chapter.

Activity 4 - routing tables 2

Routing tables are, or can be, involved to a greater or lesser extent in all areas of problem management. Explain how they come into play as each area of problem management carries out its particular activities.

You can find a discussion of this activity at the end of the chapter.

Activity 5 - network management

Suppose that the network is in a completely problem-free state up to the time at which the following alert is received at the Network Management Centre:

alert, c3, l5

Trace the operation of network management in dealing with this problem through the five stages of problem management.

You can find a discussion of this activity at the end of the chapter.

Activity 6 - fault handling

A similar system can be constructed for the automatic management of faults occurring on the computers of the network.

Each computer can be in one of the two states: in-service or out-of-service.

Computers can send an alert about a neighbouring computer. The alert takes the form:

alert, C, NC

which indicates an alert from computer C concerning its neighbouring computer, NC. All alerts are sent to the Network Management Centre, and this is where the expert system is located.

The same network as above is being managed so the knowledge about the configuration remains the same. Determine and represent the new knowledge needed for the state of the computers on the network and for handling faults on these computers.

You can find a discussion of this activity at the end of the chapter.

Activity 7 - computer failure

The other concern of the network management system is to deal with the problem of computers that either fail or are disconnected from the network without authorisation. One way to detect such an occurrence is for the computers on a network to monitor their neighbours and note the time since a message was last received from each neighbouring computer. It might then be reasonably assumed that a computer has failed if no message has been received from it after some sufficiently long time, T. When this happens, a monitoring computer sends an alert to the NMC. If computer_2 has received no messages from one of its neighbours in the assigned time, the alert would take the form:

alert, computer_2, no_messages.

Devise a means by which the NMC may detect failed computers. Again, describe the complete management process.

You can find a discussion of this activity at the end of the chapter.

Review Questions

Review Question 1

The network management scenario can be described as the network-under-management connected to a Network Management Centre. Information flows from the network to the Network Management Centre. How can this information be characterised in its totality?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 2

Following on from Question 1, during network management what flows from the Network Management Centre to the network?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 3

Given that the information flowing from the network to the Network Management Centre is consolidated in a database, what is the essential difference in what happens during manual network management and automatic network management?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 4

How can a network management system deal with the situation that arises when a link in a network develops a fault?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 5

What would happen if a message were sent to a computer with a full input queue? How could this be prevented?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 6

Devise a routing table for computer 3 in the little network illustrated above. Change the table in a way that allows it to respond to the situation when computer acting as the intermediary between computers 3 and 2 is busy.

You can find an answer/comment for this review question at the end of the chapter.

Review Question 7

How could the fault management system deal with a faulty link in such a way that the fault is not apparent to the users of the network? How could it deal with a failure to a computer providing a specific resource?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 8

What would be a suitable performance management strategy for a network that aimed to treat all its users equally, and to deliver the messages offered to it as quickly as possible at all times?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 9

What kind of thing could happen to a network that did not take care of its own security because it failed to provide security management?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 10

To clarify that the classes of network management correspond to problem management, cast them all in a form such as: 'fault management is the management of the problems that arise in diagnosing and dealing with faults'.

You can find an answer/comment for this review question at the end of the chapter.

Review Question 11

What is an alert? Why is one sent? Where is it sent to?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 12

After the alert:

alert, computer_25, neighbouring_computer

has been sent, a cluster of associated alerts will also be sent. From where will they originate?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 13

The alert:

alert, computer_7, no_service

indicates that computer_7 is complaining about a lack of service from a resource. After this alert has been sent, a cluster of associated alerts will also be sent. From where will they originate?

You can find an answer/comment for this review question at the end of the chapter.

Discussion Topics

1.

2.

Answers and Comments

Activity 1

A doctor, when dealing with a sick patient, follows this procedure when ensuring that the patient really is ill, diagnosing the illness, treating it, and so on. Similarly, a mechanic dealing with a car that has developed some problem follows the same procedure.

Activity 2

It is possible to locate problems that occur consistently, either at a particular time or in a particular place. It is also possible to detect patterns of problems: this may show that some problem is not, in fact, a problem in itself but the consequence of a causal chain of other problems.

Activity 3

The network must be monitored to determine the pattern of the traffic within it. The changes to the routing tables can then be found by determining how they must act to change the current state to the desired state.

Activity 4

During fault management, references to faulty computers need to be removed from routing tables; routing tables need to be changed to route messages around faulty links and computers. During performance management, the routing tables need to be change as discussed in Activity 3. During configuration management, references to computers need to be added to and deleted from routing tables as new computers are added to the network and old ones removed from it. With accounting management, routing tables can be changed to provide priority routes for which there is an extra charge; if a fault causes a route to change with the consequence that an agreed quality of service cannot be provided, then accounting management must be informed. With security management, routing tables can be changed to ensure that messages requiring certain levels of security are routed only to secure sites; equally they can ensure that messages are not routed to non-secure sites.

Activity 5

The stages are:

1. The alert arrives, indicating that there is a problem.

2. Checking that line 5 is actually attached to computer 3 (by finding the knowledge item 'c3 is-start-of l5') ensures that the problem is not invalid. At this point, the first rule is invoked, and the state of line 5 is changed from 'in-service' to 'in-test'.

3. Now the management system must find ways to by-pass the problem so that the network continues to operate despite the fault. At the same time, line 5 is actually tested.

4. Assuming that the test result is 'ok', indicating that the line is no longer faulty, rule 2 will be invoked changing the state of line 5 back to 'in-service'. At this point, the network is restored to its proper working state.

5. An account of the management activity is recorded.

You should trace through the variations on this scenario that occur when the alert is invalid, and when the test result is 'not ok'.

Activity 6

Initially, the state of the computers can be represented by:

in-service is-state-of c1

in-service is-state-of c2

. . .

The knowledge for handling faults on the computers is:

IF in-service is-state-of NC

AND alert, C, NC

THEN out-of-service is-state-of NC

IF out-of-service is-state-of NC

AND alert, C, NC

THEN out-of-service is-state-of NC

IF out-of-service is-state-of NC

AND ok is-test-result-for NC

THEN in-service is-state-of NC

IF out-of-service is-state-of NC

AND not-ok is-test-result-for NC

THEN out-of-service is-state-of NC

Activity 7

The stages are as follows:

Stage 1 is that an alert arrives, indicating that some problem exists.

Suppose it is the alert given above. It will be followed by a cluster of other alerts. These will come from the other neighbours of the problem computer. The other alerts might be:

alert, computer_1, no_messages.

alert, computer_4, no_messages.

Stage 2 is now reached. From the cluster of alerts, the NMC can find the computer that has as its neighbours computer_2, computer_1 and computer_4, and deduce that the problem is with computer_3. (The NMC will have a description of the topology of the network, so that it is in a position to make this deduction.)

Stage 3. The management system must now work around this computer, perhaps find another computer offering the same resources, and also send a technician to fix or reconnect it.

Stage 4. When the computer has been fixed and reconnected, the management system can restore the network to its original state.

Stage 5. An account of the problem and the problem management activity is recorded in the log.

Review Question 1

The information flowing from the network to the Network Management Centre is information about the state of the network.

Review Question 2

Control signals, that is, signals capable of changing or correcting the state of the network as required.

Review Question 3

With a manual system, the person acting as network manager will interrogate the database, while with an automatic system an expert system or some similar item of software will take actions based on the contents of the database.

Review Question 4

By ensuring that no traffic is sent down that link, and by finding an alternative route for any traffic that would have otherwise been directed over that link.

Review Question 5

If a message is sent to a computer with nowhere to store it, the message will inevitably be lost. This can be prevented by monitoring the state of the queues at each computer so as to prevent messages being sent to any computer with a full queue.

Review Question 6

The routing table could be:

Destination	**Forward to**
1	1
2	1
4	4

The amended routing table would be

Destination	**Forward to**
1	1
2	4
4	4

Review Question 7

A link failure can be covered up by finding and using an alternative route to any route that involves the failed link.

If a computer providing a resource fails, this can be covered up by locating another computer providing the same resource and directing resource demands to it.

Review Question 8

One strategy would be for the network to continually try to spread the traffic evenly across the network, so that there were no congested regions and no inequitable delays to messages held up by congestion.

Review Question 9

The network could damage itself to the point that it could no longer operate by, for example, allowing the messages it carried to cause it to overwrite its own operating software.

Review Question 10

Configuration management is the management of the problems that arise as a result of changing the configuration of the network.

Performance management is the management of the problems that arise as a result of trying to maintain the performance of the network at some assigned level.

Accounting management is the management of the problems that need to be tackled in order to monitor customers' network usage and generate their bills.

Security management is the management of the problems that arise in the course of maintaining the security of the network.

Review Question 11

An alert is a way of drawing attention to a problem. It is sent because a problem has occurred. It is sent to the Network Management Centre.

Review Question 12

Alerts will come from the other neighbours of the computer that computer_25 is complaining about.

Review Question 13

Alerts will be sent by the other computers that fail to receive service from the same resource.