Micromuse,
Management & Netcool™

Document: Micromuse, Management & Netcool™
Prepared by: Mike Silvey
For: Micromuse
15818 Midway Road
Dallas
Texas 75244
Tel: 1-800-NETCOOL
Fax: 1-(214) 980 8963

Date: 20 September, 1995
Version: 1.0, Revision A

Micromuse Standard Disclaimer

In no event will Micromuse PLC be liable for any lost revenue profit or data, or for special, indirect, consequential, incidental or punitive damages however caused and regardless of theory of liability arising out of the use or inability to use the system, even if Micromuse has been advised of the possibility of such damages. In no event shall Micromuse's liability to customer, whether in contract, tort (including negligence), or otherwise, exceed the fee charged by Micromuse for the implemented solution.

Copyright © 1995 Micromuse PLC, Micromuse USA, Inc.

1. Micromuse, Management & Netcool™

1.1 Introduction

This guide has been developed as an aide to both sales, technical support staff, and prospective customers to provide a better understanding of Micromuse, and the Netcool™ range of products, the market segment they address and operate in, some of the competitive products, and where we intend to go with the Netcool™ range, and Complexity Management.

The guide can be used standalone, or in conjunction with the Netcool™ product presentations. The guide may contain information which will be of interest to organizations with competitive products so should be treated as Company sensitive. If there is information in the guide that you think may be useful as a sales tool for customers/prospects, this can be reviewed and made available by the Micromuse Netcool™ team.

Sales guides are only useful if they are readable, concise, up to date, and contain relevant information. If you have any comments on the information in this guide, please discuss them with either Christopher Dawes, Mike Silvey, or Colin Pittham.

2. Contents

1. Micromuse, Management & Netcool™ 3

1.1 Introduction 3

2. Contents 4

3. Micromuse 6

3.1 A Brief History 6

3.2 Company Profile 7

4. Complexity Management 8

4.1 Enterprise Management 8

4.1.1 The International Standards Organisation 8

4.1.1.1 Open Systems Interconnect (OSI) Connectivity 7 Layer Model 8

4.1.1.1.1 9

4.1.1.2 OSI Network Management Categories 9

4.1.1.2.1 Fault Management 9

4.1.1.2.2 Performance Management 9

4.1.1.2.3 Accounting Management 10

4.1.1.2.4 Configuration Management 10

4.1.1.2.5 Security Management 10

4.1.2 Operational Enterprise Management Solutions 10

4.2 Micromuse's Complexity Management Architecture 12

4.2.1 The Tactical Complexity Management Architecture 12

4.2.1.1 The Agents 13

4.2.1.2 Management Platform 13

4.2.1.3 Performance Baselining 14

4.2.1.4 Fault Filtering 14

4.2.1.5 Service Level Management/ServiceDesk 14

4.2.2 The Strategic Complexity Management Architecture 15

5. Other Management Concepts 17

5.1 Inclusive Management 17

5.2 Exclusive Management 18

5.3 The Benefits of Exclusive Management 18

5.4 Service Level Management 19

5.4.1 An Illustration of Service Level Management 19

5.5 Virtual Private Networks (VPNs) 21

5.6 Applied VPNs with Service Level Management 22

5.7 The Role of the Telco in Managed Network Services 22

6. Netcool™? 24

6.1 The Netcool™ Product Family 24
6.1.1 History 24
6.2 Netcool™/OMNIbus 24
6.2.1 What is Netcool™/OMNIbus? 24
6.2.1.1 A Detailed Explanation 25
6.2.1.2 Netcool™/OMNIbus and the Remedy Action Request System 27
6.2.2 Example Implementation Profiles for Netcool™/OMNIbus 29
6.2.2.1 Single Management Platform 30
6.2.2.2 Multiple Management Platforms 31
6.2.2.3 Remote Facilities Monitoring 32
6.2.2.4 Wide Area Monitoring 32
6.3 Netcool™/LegacyWatch 34
6.3.1 What is Netcool™/LegacyWatch 34
6.4 Netcool™/Messenger 37
6.4.1 What is Netcool™/Messenger? 37

7. Case Studies 38

7.1 A High Street Financial Organisation Monitoring Burglar Alarm Systems 40
7.2 A Telecomms Carrier Monitoring Its Data Network Infrastructure 38
7.3 A Telecomms Company Providing Customer Network Management 41

8. Competition and Other Noise 43

8.1 History of the MoM 43
8.2 MAXM Systems, Inc. MAXM 44
8.2.1 Overview 44
8.2.2 Technical Description 44
8.2.3 Competitive Profile 45
8.2.4 MAXM in Summary 46
8.2.5 MAXM Pricing 46
8.3 Boole and Babbage, Inc. Command/Post 46
8.4 Objective Systems Integrators, Inc. OSI-NetExpert 47
8.5 Competitive Feature Breakdown Matrix 49

3. Micromuse

3.1 A Brief History

Micromuse was formed in September 1989, by Christopher Dawes, as a Unix Systems Integrator to Corporate environments.

In 1989, Unix was quite unknown (and almost taboo) in environments other than Financial Dealing Rooms and Universities, so Micromuse was at the leading edge in delivering Unix to Corporate operations.

The Company quickly became respected for its technical skills, which were normally employed in integrating the Unix systems with legacy, or PC systems, where previously integration had been poor.

With the growth in demand for Unix in Corporate environments, came a growth in the complexity of the environments the systems were operating in. Issues included connectivity, network management and systems management and administration.

Gradually, more of the Company's time was spent solving complex networking and management problems, that Micromuse decided to focus on the area of Network Management.

In 1992, Micromuse launched Complexity Management and instantly became a leader in Network Management integration. The Complexity Management architecture was innovative and simple.

Complexity Management was founded on the principle that since open systems based networks change on a six monthly cycle, any network management environment must be capable of rapid reconfiguration and flexibility. Bespoke applications just cannot do the job.

Also, Micromuse was tracking developments of the SNMP based management platforms (SunNet Manager & HP OpenView Network Node Manager), and the wealth of compatible partner applications which were being introduced to provide network analysis, trouble ticketing, systems performance monitoring, device configuration and other functionality.

Micromuse's Complexity Management architecture defined the requirements of a management environment, then chose the best of breed component products which best delivered that functionality.

Qualifications for inclusion in the Complexity Management architecture were that the products were best of breed, configurable with little effort, and could integrate with each other. Development is not the key, strategically, identification of products and the subsequent integration of those products into a Complexity Management system is the issue.

Over the years, Complexity Management has been proved as a working architecture for network management integration - delivering functionality which was not available in monolithic products, or non-integrated Complexity Management components.

By 1993, Micromuse identified that an emerging requirement from telecomms companies and corporate organisations was for Service Level Management - the real time maintenance of Service Level Agreements SLAs) on Virtual Private Networks (VPNs).

Micromuse embarked on the development of the Netcool™ range of products, with Netcool™/OMNIbus as the flagship Service Level Management system.

Netcool™/OMNIbus was designed to deliver Service Level Management, with information from any SNMP or other Management Platforms and devices to map onto prescribed Service Level Agreements.

Netcool™/OMNIbus as a monitor of managers is covered later in this paper, but differs from other offerings in that the product is an application, not a development environment.

Netcool™/OMNIbus was launched at the Enterprise Management Summit'94 in Santa Clara, CA, at release 1.0. Release 2.0 general availability was January 1995, and Netcool™/OMNIbus version 3.0 is released on 30th September, 1995.

Micromuse now delivers its Complexity Management and Service Level Management solutions to Fortune 500 Corporations in the US, Europe and Scandinavia, and is looking to grow an Asian operation, in the future.

3.2 Company Profile

Micromuse, was established in 1989, and is the leading developer and integrator of Service Level Management products specifically for telephony & corporate environments. The company has offices in the US and Europe, providing both support and sales/marketing activities.

The personnel profile of Micromuse is split; 50% technical support, 25% sales and marketing, and 25% finance and operations. Currently, there are ~60 employees (September, 1995).

Micromuse's Netcool™ range of products provide Service Level Management to enterprise network environments.

The Netcool™ range of products have won awards for innovation in network management, such as Data Communications "Hot Product" and Managing Distributed Systems "Application Excellence" awards.

Since inception, the company has grown 50-100% year on year, with a gradual transition of major revenues from hardware to network management software, with the turnover for FY'95 being around $20M.

Revenues from Service Level Management and Helpdesk products for Financial Year 1995 will make up 50% of turnover.

4. Complexity Management

Complexity Management is an architecture for the delivery of network management solutions to Enterprise Management problems.

Enterprise Management is the all encompassing management of an organisation's IT and telephony environments. Micromuse has coined the phrase ***Complexity Management*** to describe our approach to solving the problems of Enterprise Management.

Micromuse's Complexity Management solution, which can be a combination of many products including the Netcool™ branded products, will address specific key solutions of Enterprise Management problems.

4.1 Enterprise Management

Enterprise Management problems can be divided into a number of categories, depending on the authority discussing the problem. In this document we will discuss two approaches, that of the International Standards Organisation's Open Systems Interconnect ISO OSI Management Framework, and that of the operational environment, where a real organisation has to deliver a management solution to it's varied requirements.

4.1.1 The International Standards Organisation

The International Standards organisation (ISO) is a group representing the interests of companies with a charter to provide standards (for amongst other things) computer communications and management interfaces.

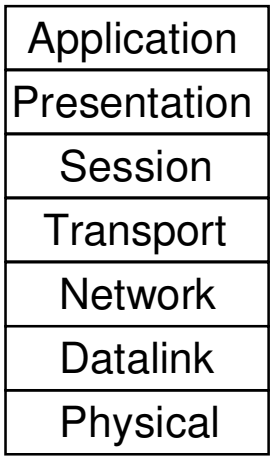
ISO has members from all the leading telecomms companies, and other computing and corporate organisations with a large investment in diverse computing and communications technologies.

The charter is to deliver published interoperable standards that any organisation can work with freely, and if the organisation is a fully paid up member of the ISO, can contribute to the standards proposals.

4.1.2 Open Systems Interconnect (OSI) Connectivity 7 Layer Model

The International Standards Organisation (ISO) has for several years been delivering standard interface APIs for the Information Technology industry to enable different types of electronic devices (computers, telephony equipment, Coke machines, etc.) to communicate with each other. These standards are called Open Systems Interconnect (OSI).

OSI defines many areas of computer systems interaction, using a seven layer model to define the various layers of interconnectivity with various API interfaces describing connectivity at each layer. The following diagram illustrates the layer definitions.



With the ISO OSI Seven Layer model, computer communications protocols have been defined to allow transparent communications and application interaction between heterogeneous varieties of computer system and networks (i.e. IBM mainframes and Unix systems).

Now that the communications standards have been defined, the ISO set about producing a set of standards for computer system network management - sometimes referred to as OSI Network Management, or CMIP/CMISE - although CMIP/CMISE are some of the actual protocol definitions for OSI Network Management, not the architecture.

The ISO first defined five categories of network management, and the next section describes OSI Network Management and the five management categories.

4.1.3 OSI Network Management Categories

OSI Network Management has been broken down into five distinct categories that the ISO believes encompasses all aspects of network management environments, for any given piece of computer equipment.

4.1.3.1 Fault Management

The Fault Management category defines all aspects of handling a fault, such as what is a fault and the types of faults you can have. This includes for our purposes, aspects of helpdesk/trouble-ticketing, fault correlation and consolidation.

4.1.3.2 Performance Management

Performance Management defines the long term monitoring of a managed object or group of managed objects. If you monitor something for a long enough period, you can establish a performance baseline that represents how the object works under different circumstances.

The more objects you monitor concurrently, the better a composite view of your network you will have, and so the better you will be able to react to circumstances because you will have seen those conditions before.

4.1.3.3 Accounting Management

Accounting Management is all about being able to use the Fault and Performance Management data to account for aspects of usage of equipment. It is not just used for billing purposes - for instance you may wish to account for the certain usage of a line to cost justify increasing the bandwidth, the same applies to the usage of a large server with respect to upgrading it. Without the accounting data, this is not really possible (only fingers in the air can help!).

4.1.3.4 Configuration Management

Configuration Management is fairly simple to understand. It defines how you interact with an object to control it, and how you maintain previous configurations, etc. Configuration Management is all about the administration of objects.

4.1.3.5 Security Management

The Security Management category defines all aspects of interaction between managed objects and management tools, such as access security authentication, encryption of data during conversations, etc.

4.1.4 Operational Enterprise Management Solutions

It's all very well having interoperability and management standards defined by an industry body such as the ISO, but sometimes, because of the complexity of the task of creating the standards, the time it takes, and the pace of change in the computing industry, these standards do not get widely adopted, or, something different comes along which takes the market by storm.

This has happened in the network management arena. The ISO OSI Network Management standards have been very slow to develop. Much of the work has been put into infrastructure as one might expect, which has meant that the detail of interoperability of the OSI management standards has come much later.

Also, much of the OSI Network Management work has gone into defining standards for the telecomms players, who are actually delivering a very complex service and need to interoperate with each other.

Because the OSI Network Management standards have been aimed at the telecomms players, the standards defined are very complex to implement, and so widespread market adoption of them has not happened.

The general market outside of the telecomms companies have chosen to implement network management environments using an Internet defined management protocol called the Simple Network Management Protocol (SNMP).

This has led to a divergence of management platforms (the application that users use), some for specific managed objects using either OSI Network Management protocols or proprietary, and the so called open management platforms used to manage SNMP networks.

Also, although the ISO OSI framework for management (the five categories) seems to define what *a* network management system should deliver, there is no single product which can provide every requirement.

In fact those applications which have tried to do everything have ended up being less than good in any area.

Since there is no single application which provides a complete network management system, integrated network management environments have to be created using *component* based applications.

Component applications are those which deliver a useful function of a network management environment, and can integrate with other applications to provide a network management solution.

Working operational network management environments will *only* be delivered by implementing a solution using many different management applications, all providing a certain function, that when integrated co-operatively delivers an integrated network management solution.

4.2 Micromuse's Complexity Management Architecture

For the past 5 years Micromuse have been integrating "open" management solutions, utilising best of breed, off the shelf components integrated from the ***Complexity Management*** architecture.

Micromuse defined both the term, Complexity Management and the block diagram architecture to enable us to present the "What we do" and position the management applications in our portfolio.

The Customer/prospect has confidence that the Micromuse Complexity Management solution can deliver tactical point management solutions, that later can be integrated with other products (from the architecture) developed from a "tactical" management solution into an enterprise management system.

Complexity Management makes it easier to implement management, by breaking down the enterprise into deliverable components that can be integrated later. In addition, the initial outlay of money can also be reduced, and thus easier to justify.

The Complexity Management architecture shows that Micromuse actually understands the problems that IT management staff and operators face, and can address those problems, without having to buy the whole system at once.

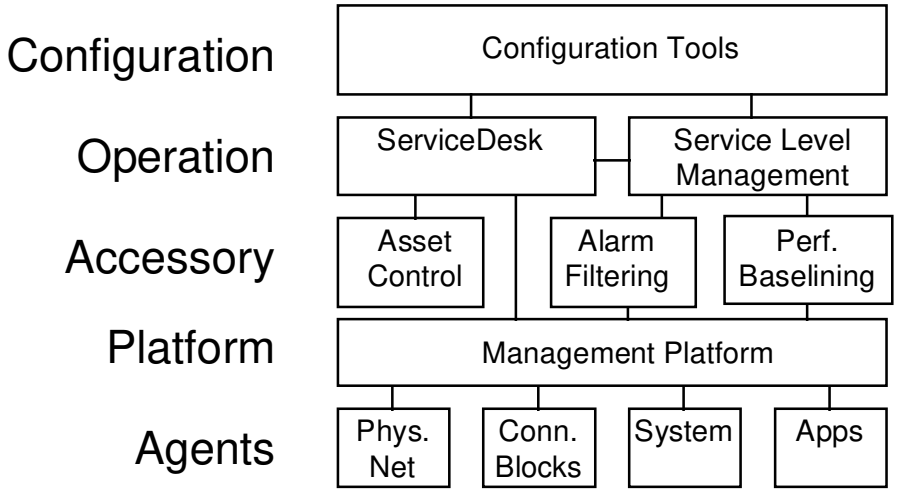
The added benefit to the customer is that Micromuse uses best of breed, industry acclaimed products (some of which we actually helped make into the names they are now) integrated together to provide the whole solution.

Its interesting but today, there are many imitators of the Micromuse Complexity Management architecture - such as AT&T GIS with their OneVision program - although OnVision has some fundamental architecture misfits.

4.2.1 The Tactical Complexity Management Architecture

Micromuse has defined the Complexity Management architecture to be independent of any particular network management platform. Although in reality, with the products in our portfolio from US vendors, the main management platforms to work with will be those from Sun, Hewlett-Packard, and IBM, since most of the products were designed to work with these.

The Complexity Management architecture defines a number of interconnected blocks (or categories) which allow us to deliver much functionality described by the five OSI Network Management categories.



The Tactical Complexity Management Architecture

We have chosen the best of breed products for each category, making sure that different applications in the categories can talk to each other in a logical way which allows an integrated network management system to be developed. Into each block of the Complexity Management Architecture, our customers can either put their favourite product, or use one of our "best of breed" choices.

4.2.1.1 The Agents

At the base of the architecture we have the agents - categorised into the PHYSICAL NETWORK; mainly RMON LAN and WAN probes, CONNECTIVITY BLOCKS; meaning the blocks that connect networks together - routers, Hubs, bridges, switches, etc., SYSTEMS; agents which provide for the management of operating systems such as SunOS, Solaris, AIX, Windows NT and Novell, etc., and APPLICATIONS; applying to databases, and other applications which need managing (i.e. Reuters Triarch).

At the Physical Network agent level, Micromuse provides Frontier NETscout and HP NetMetrix, no agents are provided by Micromuse for the Connectivity Blocks because most of them today are equipped with SNMP agents. At the Systems level, Micromuse supplies Landmark Systems TMON for Unix, and IBM's Systems Monitor (for use with NetView for AIX under certain circumstances), and at the applications level Micromuse currently supplies BMC Patrol (although there are several SNMP agents on the market for Database management).

4.2.1.2 Management Platform

Next block is the MANAGEMENT PLATFORM. In most cases we are normally referring to SunNet Manager, HP-OpenView Network Node Manager, or IBM NetView for AIX (and Solaris).

Equally apply this category to your favourite network management platform (Cabletron SPECTRUM, Network Managers, NetLabs, SMS, Novell/NMS, etc. [forgive me if I miss one out!]).

Generally we would recommend only using the platform as a hub for gathering network fault and performance information from the managed objects, since most of the platforms

on the market are both not truly multi-user (with authentication etc.) *or*, support fault correlation...and in addition, they do not integrate well with other like/unlike management platforms (but of course they all promise this in the future!!!).

Micromuse supplies SunNet Manager, Sun Solstice Enterprise Manager, HP OpenView Network Node Manager (NNM), and IBM NetView for AIX.

4.2.1.3 Performance Baselining

At the next layer, we are looking at tools to enhance the (lacking) functionality of the management platforms. Firstly, network managers should be addressing PRE-EMPTIVE management, not just PRO-ACTIVE management, i.e. identifying that the problem is going to happen before it actually happens, not after(!). To do this you need good PERFORMANCE BASELINING of your managed environment to both profile the performance of the internetworked elements, and to identify the "whys?" of breakdowns of parts of the network environment. In other words, see what failed when, and what other components may have caused the "what" to fail, *and then*, identify the prevailing conditions which led to the failure of that item...allowing
the organisation to set up some FAULT FILTERING.

Micromuse has historically sold Remedy's Health Profiler into this category, although recently this product was discontinued. We still discuss this category, although we are at present without a product.

4.2.1.4 Fault Filtering

The popular management platforms don't do FAULT FILTERING too well (some would say "not at all!"). Most administrators have spent an awful long time setting up their management platform for both Trap handling, and Event polling for specific conditions - then unfortunately meet with the problem that there is no Event de-duplication (i.e. a fault condition generates multiple notifications or traps), or Event/Trap Correlation (i.e. the ability automate: if this and that happen at this time, alert me).

Micromuse provides Netcool™/OMNIbus to do this.

4.2.1.5 Service Level Management/ServiceDesk

Above these tools comes both SERVICE LEVEL MANAGEMENT, and SERVICEDESK. The two are very separate and extremely compatible, and almost self requiring of each other. The Service desk is used by the back end support teams for management of the fault process/escalation etc., and the Service Level Management element is used by the support teams for real-time monitoring of Service Level Agreements and Virtual Private Networks.

Service Level Management applications should provide correlation, multi-user access to management applications and information and use an Exclusive Management paradigm.

Micromuse provides Remedy's Action Request System for the Service Desk, and Netcool™/OMNIbus for the Service Level Management.

4.2.2 The Strategic Complexity Management Architecture

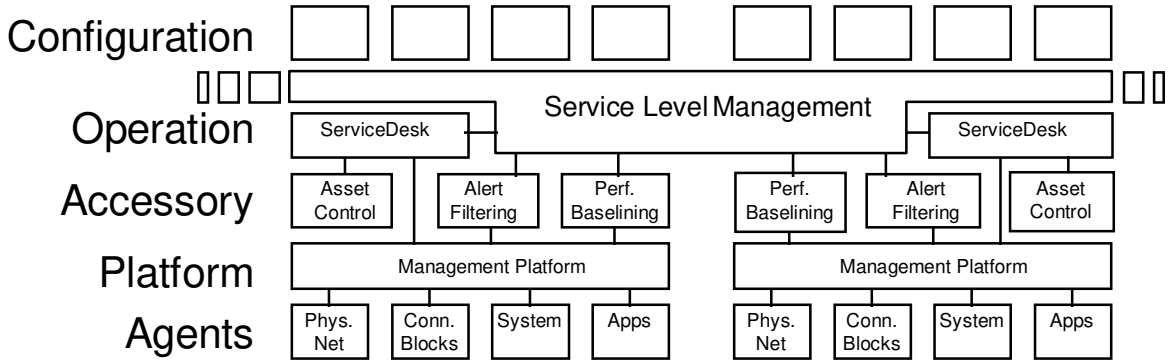
We refer to the architecture defined in section 4.2.1 as a Tactical Complexity Management environment (or Tactical Domain), because it only deals with a single management platform environment.

Most of the larger organisations who really understand that they have the need for a Complexity Management environment and products, have more than one management platform, and these platforms are normally different to each other, such as a platform for SNMP management, and other platforms for mainframe and telecomms environments.

These organisations require a strategic Complexity Management environment which can consolidate many separate tactical Complexity Management domains into clients of each other.

The following block diagram shows the strategic Complexity Management environment. The service which pulls all the tactical domains into a consolidated structure is the distributed Service Level Management system.

The Service Level Management system is the application which can pinpoint Virtual Private Network failures and SLA dependency failures around the network from different management platforms and then provide the correlated information to those who need to know it.



As an illustration of how the tactical domains can work strategically, take as an example an organisation with a WAN telecomms department using their own management environment, a LAN department managing their systems using a popular SNMP management platform (i.e. SunNet Manager, HP-OpenView NNM, or IBM NetView for AIX), and the systems department using another copy of one of the popular SNMP management platforms.

Management at this organisation is done from a central site at head office, but all the groups are separate. This means that a fair amount of remote management is being done to other buildings via the WAN. The different departments have to use different management systems because the tools to manage them are different and require their own platform.

If one of the WAN links fails, and a fallback link does not come up, the following could happen, faults begin to be detected from all the networking equipment at the remote sites by the LAN management group, the systems group (who are perhaps only monitoring their critical servers) receive faults from their server, and the WAN group is informed by their management system that one of their links is down.

So, in this case, the three different groups of personnel would all start to work on the problem (the problem of course that is simply to do with the WAN group).

This is because they do not have the fault information from the different management platforms consolidated together, which would then allow them to create automation rules such that if the WAN link to a site failed, the LAN support and Systems support personnel would be notified with a message saying that their equipment is in an unknown state because of a failure currently being handled by the WAN support group.

Strategic Complexity Management Environments are created by using a multi-platform, multi-user, fault management environment.

5. Other Management Concepts

This document covers a description of management environments, some key components of those management requirements, and some of Micromuse's own products to address key environments and organisational needs.

To best explain the features and technological lead of the Netcool™ products, some management paradigms must be discussed. The following explains; Inclusive and Exclusive Management, and why Exclusive Management based products will always be superior, Service Level Management, and Virtual Private Networks.

This section should give readers an idea of what aspects of management are important, and where the future of management environments are taking us.

5.1 Inclusive Management

Inclusive Management is a term used to describe the way some management systems work. Some management environments which attempt to provide "intelligent" fault management utilise the Inclusive Management paradigm.

This is where all faults from the environment are consolidated, then intelligently processed using a management application - the aim being to centralise the alarms stream, then using complex rules based correlation, and a "model" of the enterprise environment, only show alarms representing the real problem, rather than, perhaps, hundreds of seemingly un-related alarms.

With an Inclusive Management environment, implementors of the management environment are forced to, firstly, create a database model of their environment: that is, all the equipment in the environment, and its connectivity and relationships with other equipment; secondly, apply rules to the model which represent how the network works (i.e. program in the correlation about fault relationships based on operator knowledge).

So, the Inclusive Management model includes rules for *all* the fault relationships that the support operators in the enterprise *know* about. It does not include support for the faults that the support operators *don't know* about.

The means that the system will only show the faults operators know about - whereas, the faults that are really critical to support staff are the ones they don't know about - with Inclusive Management, they never see those faults.

Inclusive Management appears like a good idea, until the purchasers of the management environment realise that it will take at least 6-9 months to create the model (in an average sized corporate IT network).

In most corporations today, the network and infrastructure equipment is normally being changed either on a continual basis, or at least every six months.

Since Inclusive Management takes longer to model the network than the rate of change of the network itself, the Inclusive based management environment never actually becomes operational, and worse than that, it's model database always looks like a history of how the network was, rather than what it is like today.

Inclusive Management based projects tend to generate large volumes of consultancy for the vendor, take a long time to pass the planning/development stage, and invariably do not reach operational delivery. (There is also the issues of getting the network, systems, telephony, and applications support operators to reveal all they know about the contexts of failures).

Products in Inclusive Management category include OSI-NetExpert, and to a lessor extent, MAXM, and Command/Post. Inclusive Management products tend to be development environments that can be programmed, and thus require large consultancy projects.

5.2 Exclusive Management

Exclusive Management, is, as you would expect, the opposite of Inclusive Management.

Similarly to Inclusive Management, Exclusive Management consolidates alarm feeds, and allows filtering and correlation to be applied, except that in the Exclusive case, no model or rules are required for the system to become operational.

Exclusive Management works on the principle that the system should be operational quickly, with minimal programming/scripting/modelling and allow correlation to be built "*on the fly*".

Exclusive Management sends *all* alarms to the operator, allowing the filtering out or correlation of alarms that are known about, leaving the critical alarms that are unknown.

Exclusive Management allows the real time creation of correlated rules, based on actually seeing the alarms in an EventList. Thus when implementing an Exclusive based system, there is no reliance on the memory of the experienced support personnel, operators see the alarms as they happen.

Not only is Exclusive Management much quicker to implement, but it is also easier, allowing more junior operators to configure rules as the events happen - thus allowing the experienced operators to get on with solving complex projects.

An example of an Exclusive Management based system is Micromuse's Netcool™/OMNIbus Service Level Management system. Exclusive Management systems tend to be product based, which are working as soon as they are installed and added functionality can be configured rather than programmed.

5.3 The Benefits of Exclusive Management

The benefits of Exclusive Management over Inclusive Management are obvious to most operations, support, and experienced management personnel, but in detail are as follows:

- Implemented and operational in days rather than months
- Correlation relationships can be added/changed in real time
- Is not intrinsically reliant of experienced operator knowledge
- Actually delivers a service which is useable operationally
- Maps quickly and easily as the network infrastructure changes
- Works in real time
- No programming or scripting required to change or add functionality
- Delivers historical Uptime, Downtime and %Availability across managed entities

An Exclusive Management system can be demonstrated OnLine in real-time - and proves useful right out of the box. It is an application rather than a development environment.

5.4 Service Level Management

Services are “Applications” which can be isolated and managed. A Service includes a diversity of telephony, physical cabling, systems, applications and networked nodes, arranged as a logical grouping to represent a usage profile,

i.e. A **Department** - all the IT equipment in that department as a single managed entity, *or* an **Application** which is client-server, working over a distributed network between a number of servers - if any of the items connecting the servers, or the servers themselves fail, then the Service should be seen to fail.

A Service can be distributed geographically and across a large variety of an organisation’s computing resources - therefore also across a large number of management platforms covering different areas of the IT infrastructure.

When a Service has been identified and a Service Level Agreement (SLA) is in place, Service Level Management will maintain the Service within the prescribed envelope of performance determined the SLA.

Another term for the Service, is a Virtual Private Network.

5.4.1 An Illustration of Service Level Management

The following is a graphical illustration of how Service Level Management maps the way an organisation works.

In most organisations, each strata is managed by separate departments, Mainframes and Mini’s by the Datacenter, PC LANs are often managed at a departmental level, Unix sometimes the same or by the Datacenter.

The Hubs, Routers, Switches etc. Are normally run by the Network group, and all telephony and WAN services are run by the Communications or telecommunications department.

(We could add Applications, Physical, and other strata, but in the main this covers the equipment and technologies).

Most organisation have either management platforms, or console “bridges” into their important equipment and services to provide a view to status of the equipment.

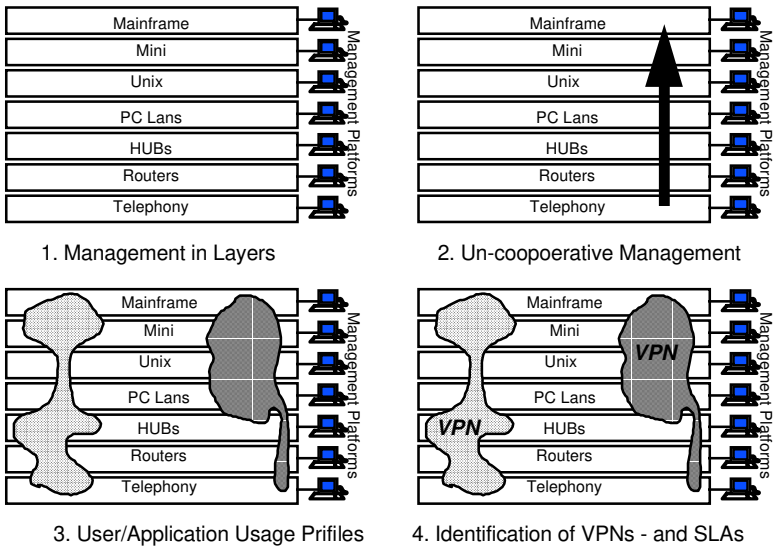
For the mainframe/SNA; Host NetView or NetMaster, for Mini Computers; normally consoles, DECmcc, or NetMaster, Unix; OpenView, NetView AIX, Patrol, EcoTools, or TMON and Tivoli or Unicenter.

Management of PC LANs is normally provided by the network technology vendor - i.e. NT; SMS, NetWare; Novell/NMS, etc.

Hubs, Routers, Switches, and other SNMP based equipment (if an organisation is serious about this) is managed by either the Unix variant of OpenView (Network Node Manager),

SunNet Manager, or NetView for AIX. Other prominent systems are DEC PolyCenter NetView, & Cabletron SPECTRUM.

To manage telephony equipment, the management software is provided by the vendor, for example; Stratacom, Ascom Timeplex, Newbridge, NET, etc. All have their own management platforms - some of these companies are adding SNMP support.



The four figures (above) profile the IT infrastructure of a typical corporation, arranged as layered strata. Each of the strata are managed by separate groups or departments.

Hubs and Routers have been separated, because in a geographically dispersed corporation, there will probably be more than one management system for the internetworking equipment, thus it is easy to organise the management of single equipment types than have many arranged together.

Figure 1. Shows the strata, and that each layer has a management system or console into its equipment specialism. This shows the typical management profile. If an organisation is managing in this way, this is good.

If the mainframe has an fault, the mainframe management system will present an alarm to that support group.

If a Router has a fault, the network support team supporting it will receive and alarm.

The same is true for all the layers - therefore we do have management!

Figure 2. Shows that although we have management at each of the layers, if we have a problem at a layer which is supporting other layers above it, the fault may cause “phantom alarms” in other strata.

An example phantom alarm may be cause by a failure of some internetworking component in the Telephony strata. If this equipment fails, alarms may be generated throughout other strata which appear to have no relation to the original fault.

Support personnel in the other layers may spend time trying to fix the phantom alarm, only to find that the original cause was with the Telephony.

Phantom alarms cost time, money, and personal relations between support departments.

So Figure 2. Is showing that the conventional co-ordinates for management do not provide the most effective means for support co-operation in the IT department.

Figure 3. Profiles the usage of the IT infrastructure by either applications, people, or departments.

It is unusual for a user or department to only use equipment managed in a single strata (i.e. one equipment technology). Most users and particularly departments utilise equipment across the IT infrastructure - whether by design (i.e. they have Unix and PC's on their desktop), or through the applications they use, which can be distributed across the mainframe, Unix, mini's, and with a PC based Windows frontend.

In the case of distributed applications, these will invariably be using communications links and other services.

So Figure 3. Is showing the usage profile of either a single user, a department, or maybe an application, across the IT infrastructure.

As discussed in Figure 2., the co-ordinates of management (i.e. in layers) do not map to the profile of IT infrastructure usage.

Figure 4. Is showing usage profiles described as Virtual Private Networks (VPNs), perhaps to defined Service Level Agreements (SLAs).

Figure 3. Discussed the usage profile of a department/user/application. Figure 4. Shows that these usage profiles can be viewed as Virtual Private Networks.

If the IT department has to provide support to it's customers, one department may require a support agreement with SLAs that define 7/24 support with zero downtime for its VPN, a second department may require 8/5 support but can live with 3 hours downtime.

The normal means of management (i.e. in strata layers) cannot support VPN type management to agreed SLAs.

What is required is a Service Level Management system that can utilise the information from the existing IT management infrastructure, and map VPNs to SLAs - then monitor SLA compliance in real time. The provision of historical reporting on Uptime, Downtime, and %Availability for the components can be used to provide reports to the customers.

5.5 Virtual Private Networks (VPNs)

Virtual Private Network (or VPN) is a phrase that is used in many ways. For our purposes, and in the main, a Virtual Private Network is an network that belongs to an application, service, or an organisation, which is part of a physical network, but can be isolated as a deliverable service and monitored in the same way.

A Virtual Private Network could be some Frame Relay, ATM, or IP Router network service purchased from a telecomms supplier. To the telecomms supplier, the customer is simply one user of many using the physical infrastructure. To the customer, their VPN is completely isolated from any other customers of the telecomms supplier - as far as the customer can see, they have purchased an isolated network.

Another type of Virtual Private Network may be something as simple as an application or service within an organisation. The application may utilise several disparate layers of the IT infrastructure, i.e. a financial data feed, where the application uses many Servers, and sub-Servers, telephony lines, specific ports on hubs and Routers, and Desktop workstations delivering the Service.

The data feed is one Virtual Private Network, although it is utilising elements and services which are shared by many other VPNs on the network (the hubs, Routers, Systems, Physical Network infrastructure, and telephony).

If any element in the VPN fails, then the Virtual Private Network as a whole can be seen to fail, rather than simply looking at an unrelated element failure in the network as a whole. A single element failure may cause several VPNs to have failures, meaning that we can now isolate views for many services from a network made up of many disparate and apparently unrelated elements.

Virtual Private Networks can be purchased from telecomms companies, or isolated service delivery channels in a managed IT infrastructure.

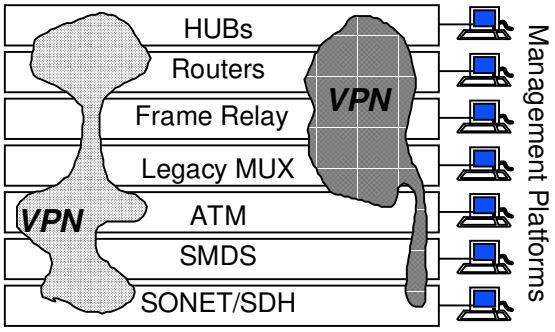
5.6 Applied VPNs with Service Level Management

Since, as described in section 3.5, Virtual Private Networks can represent any Service, and Service Level Management is the maintenance of a defined Service Level Agreement, any Virtual Private Network can mapped to a defined Service Level Agreement, and monitored in real time.

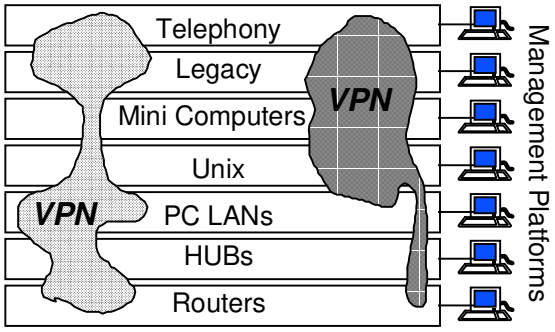
An organisation can describe any Service Level Agreement, map it to a Virtual Private Network profile, and then manage the VPN using Service Level Management.

The following illustrations show how Virtual Private Networks can be used to describe both Services provided by a telecomms company to a corporate customer in the form of a network, and how the IT department of a corporation can provide the same in terms of IT services, spanning applications, users, and departments/divisions.

Virtual Private Networks describe the Services provided by one organisation/department, to another - these VPNs can be very simple, or span multiple technologies and equipment.



The Telecom Supplier



The Corporate IT Operation

5.7 The Role of the Telco in Managed Network Services

In the future, it is becoming apparent that should a customer require a network, they will no longer purchase the equipment and build and maintain their own equipment. They will simply call a telecomms supplier, and that organisation will implement a network for them.

The network that is created can be made up of private equipment at the customer site, and Virtual Private Networks supplied over the telecomms company's own network equipment provisions.

The customer will define a requirement specification, and Service Level Agreement for the network. The telecomms company will manage this service using Service Level Management.

The telecomms company will be providing Virtual Private Networks to the customer corporation, and the infrastructure operations in the corporation will provide network, systems, and applications Virtual Private Networks to their customers in the organisation, which are subject to their own Service Level Agreements.

Service Level Management is the linking factor for all operations management of Virtual Private Networks, and corresponding Service Level Agreements.

6. Netcool™?

Netcool™ is an official brand name trademark developed and owned by Micromuse. The Netcool™ branding is used for any product that Micromuse has designed and developed - i.e. not for products such as Remedy Action Request System which is subject to a reseller contract and is part of the Complexity Management portfolio.

6.1 The Netcool™ Product Family

Today there are three Netcool™ branded products, all of which are related to each other at this time (although there may come a time when one Netcool™ branded product does not interact logically with another):

Netcool™/OMNIbus, Netcool™/LegacyWatch, Netcool™/Messenger

6.1.1 History

Micromuse's policy towards delivering Complexity Management products has been to identify products and technologies, integrate them together and therefore provide a management solution that is effectively off the shelf using standard components.

A lot of good management products exist which address a large spectrum of the features required by customers. The Micromuse view is that there is no point developing applications for the sake of it if they exist already, our skills are better used in identifying those products and integrating them.

Micromuse initiated development of the Netcool™ range of products when we identified that customers requirements did not match products that either existed, were under development.

Some tools did exist, but those were not appropriate for the type of management environment Micromuse's Complexity Management architecture is designed to address - i.e. a deliverable working management solutions that can be managed and maintained by customers.

Consequently Micromuse created the Netcool™ range of products and implemented a policy of continual customer involvement.

The Netcool™ range of products will always be ahead of the market and any "competitive products" because we listen to our customers, and have a team of management specialists whose job it is to think solutions ahead of their market demand.

6.2 Netcool™/OMNIbus

Netcool™/OMNIbus is a client-server, Service Level Management , configurable application which transforms tactical horizontal management infromation into vertical business and Service oriented management information.

6.2.1 What is Netcool™/OMNIbus?

Netcool™/OMNIbus is a client-server configurable application providing Service Level Management. Service Level Management is the real time maintenance of a Business Unit or Service (Virtual Private Network) within a prescribed envelope of performance (SLA).

Functionally Netcool™/OMNIbus *automatically* consolidates and de-duplicates fault information (Events and Traps) from SNMP, Telephony, Systems & Legacy Network Management Platforms and devices, into a clear coherent noise free information database, which displayed to the operator Desktop.

Netcool™/OMNIbus allows Boolean correlation and automation to be applied to the information. Filtered information is then presented to users via the intuitive graphical Desktop tools, which are security authenticated.

Netcool™/OMNIbus utilises existing management platforms in the organisation, protecting the infrastructure investment, allowing horizontal management environments to be viewed as a whole.

Netcool™/OMNIbus transforms tactical management domains into a strategic management environment.

The Netcool™/OMNIbus Desktop Client suite of tools provides all configuration, administration, and operator functionality from an intuitive graphical interface. No programming or scripting is required to implement correlation and automation, full functionality is provided using “drag and drop”.

The product can be installed *and* operational in days rather than months thanks to the use of an *Exclusive* management paradigm and has bi-directional interfaces to standard trouble ticketing systems such as Remedy Corporation’s Action Request System.

Netcool™/OMNIbus can integrate any SNMP, Telephony, Systems of Legacy equipment using standard software “Probes”.

Netcool™/OMNIbus is available on multiple hardware and operating system platforms, and takes full advantage of kernel multi-threading in Solaris 2.x.

6.2.1.1 A Detailed Explanation

Most organisations are run on a business unit basis, the Finance Dept., the IT Dept., the Production Dept., etc. whereas general systems and network management products work with a horizontal approach - i.e. one management system might monitor the mainframe, another might manage part of an organisation’s telecommunications and LAN environments (and an organisation may have many of these management platforms), then there may be several systems and PC management products. (*See Service Level Management*).

The horizontal management approach does not allow organisations to manage from the business unit (or Virtual Private Network) grouping - in other words, the Finance department may be using cycles from the Mainframe, various parts of the telecommunications and LAN environments, some of the Unix servers and many of the PC LANs, but horizontal management cannot encapsulate this.

Today’s management tools do not allow us to monitor the health of the Finance department, or to isolate many individual Service Level Agreements and monitor them in real time from the same product. This is the functionality provided by Netcool™/OMNIbus.

Netcool™/OMNIbus allows horizontal management information from point management platforms to model the way the business works - providing a full service level management paradigm. Netcool™/OMNIbus utilises the existing management platforms in an organisation, protecting the infrastructure investment - with Netcool™/OMNIbus, we can accurately (and reliably, based on the management infrastructure in place) monitor the health of service groupings or departments, the way a business is run.

Netcool™/OMNIbus is a shrink wrapped, client-server, configurable application providing Service Level Management. Netcool™/OMNIbus can be implemented in days rather than months. Once the system is installed, it is working, providing consolidation and de-duplication of fault data automatically, and allowing correlation to be created in real time using drag and drop.

All aspects of the Netcool™/OMNIbus system, from the cross platform Boolean fault correlation, to the administration of users and access permissions can be configured using the graphical interface which has advanced "drag and drop" accelerators.

Netcool™/OMNIbus is "shrink wrapped", building on existing management systems, utilising existing management skills and can be deployed in a few hours, even in large enterprises.

Netcool™/OMNIbus is a true multi-user system, having a suite of graphical Desktop tools for users and administrators. The system employs multi-level security authentication which allows access to views and *partner* tools to be granted on a per-user basis.

Netcool™/OMNIbus "Gates" provide dynamic data interfaces to external applications such as Helpdesk systems (Remedy Action Request System and Legent/Paradigm) and historical databases such as Sybase and Oracle.

The powerful fault distribution and multiple management domain technology of Netcool™/OMNIbus allows support staff across an organisation to select views of local or global fault status for the entire network. In addition, alerts by exception can be monitored on one site and dealt with in another, allowing critical faults or faults occurring outside normal business hours to be routed to alternative support centres.

- Delivery of real-time Service Level Management of SLAs
- Consolidates faults from all management systems
- Distributes fault information from existing management systems to staff across the enterprise
- Transforms fragmented 'tactical' domains into coherent 'strategic' management domains
- Allows Virtual Private Networks to be monitored
- Sophisticated filtering provides views customised to individual user requirements
- Provides a single (multi-user) tool to view network status and launch other management applications with full security authentication
- Builds on existing systems, installed base, and expertise
- Enterprise scale solutions can be installed and be productive in hours using shrink wrapped plug and play design
- Multi-domain management using peer-to-peer, hierarchical and web topologies
- Incorporates high performance distributed ObjectServer technology
- Implemented using open protocols. Real-time data available to other applications
- Automatic Journalling User Profiling and Notation
- Standard links into foreign applications such as trouble ticketing and historical database

If you ever need a mission statement for the Netcool™/OMNIbus system, it is to deliver correlated enterprise wide fault information providing multi-user authenticated access, but require no computing skills to configure or maintain the system (i.e. ease of use is our primary concern), while delivering the functionality described by our users.

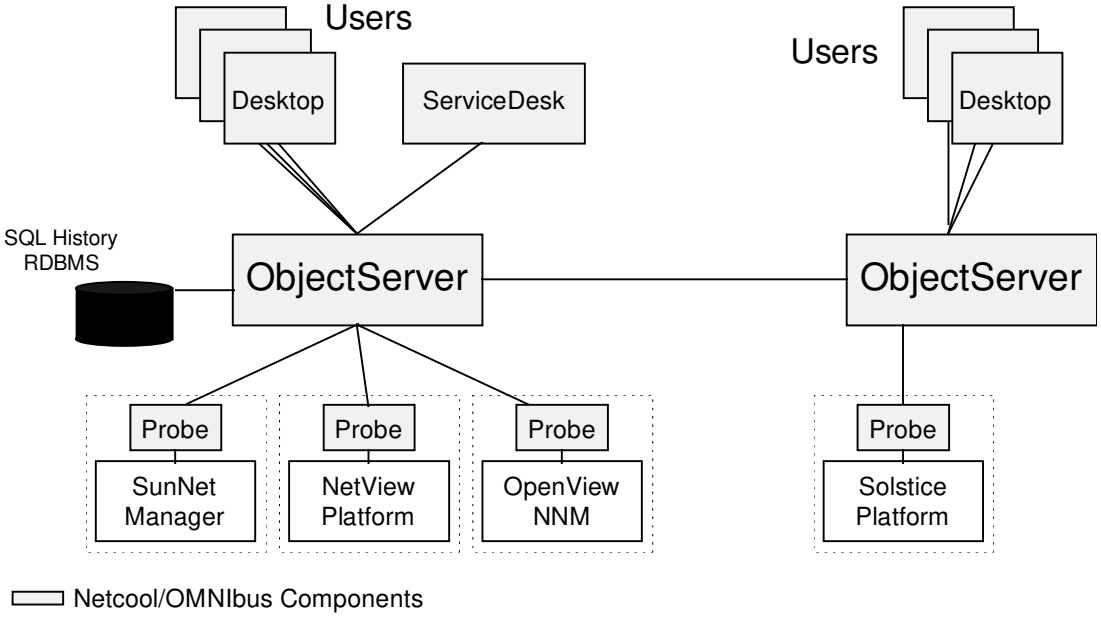
6.2.1.2 Netcool™/OMNIbus and the Remedy Action Request System

Netcool™/OMNIbus integrated with Remedy Corporation's Action Request System provides a tightly coupled fault information/escalation solution.

Not only can Netcool™/OMNIbus filter and correlate faults from multiple network management platforms, but it can also create trouble tickets in the Action Request System based on certain graphically defined conditions, i.e. on the third occurrence of a condition, create a trouble ticket - and reflect the state of the helpdesk problem in the Netcool™/OMNIbus desktop tools.

Integration between Netcool™/OMNIbus and Action Request System is fully bi-directional, allowing users of the Netcool/OMNIbus desktop to instantly view which users are assigned to which faults, and the current status of the fault. Relationships with other faults in the Netcool™/OMNIbus system can also be changed based on the current status of activities in Action Request System.

The Netcool/OMNIbus-Action Request System Gateway is an integral part of the Netcool™/OMNIbus fault information management system.



The Netcool™/OMNIbus Architecture

The diagram above shows the architecture of the Netcool™/OMNIbus system. Essentially there are three components; **Probe**, **ObjectServer**, and **Desktop**. At least one of each is required to have a working system.

The Netcool™/OMNIbus Probe collects all fault data from the management platform (i.e. SunNet Manager or HP-OpenView NNM) and forwards it to the ObjectServer. The name “Probe” can sometimes be confusing to prospects who think of a Probe as a separate piece of hardware (like an RMON Probe). The Probe is actually a software module which is installed and runs on the same hardware as the management platform that it gets its fault information from.

Probes do nothing more than get fault data from a management platform and forward this in the correct format to the ObjectServer - but the Probe is the item of the Netcool™/OMNIbus system that makes it *shrink wrapped*. Because the Probe forwards all data as soon as it starts running, it means that users see consolidated fault information from multiple management systems instantly. This is very powerful and nobody else can do this.

There are many Probes in the Netcool™/OMNIbus price list. It is our aim to have a Probe for Netcool™/OMNIbus for every management platform that our users require, and these Probes should be on the standard Price list, therefore, if the customer has a management platform that we have not already produced a Probe for, Micromuse will develop a Probe into that system and only charge the customer the list price of that Probe, not for the development work. The new Probe is then added to the standard price list.

The Netcool™/OMNIbus ObjectServer is the heart and soul of Netcool™/OMNIbus. The ObjectServer receives a continuous fault stream from many Probes, de-duplicates multiple occurrences of the same fault, consolidates faults from multiple Probes together, and correlates the information into meaningful records of the state of individual or related parts of the network environment.

The ObjectServer is an ANSI compliant SQL (Structured Query Language - as in Oracle, Sybase, et al) database that runs in real-time in memory. A memory resident database allows the Netcool™/OMNIbus ObjectServer to be extremely fast (on some systems handling thousands 000's of alarms per second).

The ObjectServer runs under SunOS, Solaris2.4, HP-UX and AIX (under Solaris2.4 the system is fully multi-threaded making it efficient and fast).

All faults from the environment being fed in by the Probes are handled here. Because the ObjectServer handles all fault information as it happens, and can do correlation, the data generated can be stored in a history database (requires Sybase or Oracle) which will then contain information such as *Uptime*, *Downtime*, and enable figures like *%Availability* of networked entities and Virtual Private Networks to be derived - all without the need or any additional collection of data.

Configuration of the automation rules inside the ObjectServer is handled as SQL scripts and sequences, *but* users never need to learn a scripting language because the configuration of the Netcool™/OMNIbus system is all handled using graphical tools with Drag and Drop capability.

The Netcool™/OMNIbus Desktop is the suite of tools that the operators and administrators use, and generally this is what the think of as Netcool™/OMNIbus - it hides all the complexity of the application with a very intuitive simple to use GUI.

The Desktop provides access to all functionality of the Netcool™/OMNIbus system without the users having to resort to the character command line editor and SQL scripting for configuration.

The Desktop is split into two clear parts, Administration and Operator. The Administration user has tools to add new users, configure views for users, and create automation rules. The users who are running the network management environment have multiple filtered EventList applications and the ObjectiveView graphical topology tool.

The EventList gives a real-time line by line text based view into single and correlated faults on the network. From an event a context specific menu can bring up the tools (from the management platform) which will allow the user to reconfigure the managed object, i.e. if a Cisco router fails, launch the CiscoWorks tool to reconfigure this. This menu is subject to the security rules so, one user may have access to all the tools whereas another user may only be authorised to view the faults in the EventList.

The ObjectiveView allows a topology to be developed with multiple viewing windows, but unlike conventional management platform topology maps. Firstly, the ObjectiveView can have several maps with access right security, *and* the fact that an icon is flashing could mean that a particular scenario has happened - Icons can therefore have fault relationships applied to them, i.e. for the management of a system, the fact that CPU% Utilisation is at 99% does not matter, but what does matter is if CPU% Utilisation = 99 AND Memory is full - so only flash the icon (or take a corrective action) when the combined state occurs. This is not possible with the "standard" management platforms.

6.2.2 Example Implementation Profiles for Netcool™/OMNIbus

Netcool™/OMNIbus provides functionality that is not available from other products, the buzzwords which will interest the customers are as follows:

- Correlation

- Consolidation
- Automation
- Multi-user (with authenticated Security)
- Installed and Operational in Days
- Client Server
- Distributed
- Protects existing infrastructure investment
- Helps define Management of Virtual Private Networks
- Delivers Service Level Management of SLAs

Correlation means that multiple faults from multiple managed objects from multiple management systems can be related together to show users what the actual fault is.
Consolidation allows fault data from multiple management platforms of any kind to be consolidated into a single environment.
Automation allows scheduled, proactive and reactive actions to be taken on the correlated fault information.
Multi-user provides views into the system to see the same or enhance information for many people concurrently, and having security authentication allows different users to have access to tools and services in a controlled manner.
Shrink Wrapped means that the system works as soon as it is installed - data is being presented to the users with no configuration required. All that's needed is a Probe, ObjectServer and Desktop running.
Distributed functionality of the Netcool™/OMNIbus system allows for scaleability where remote sites need linking together, and for different personnel to have views specific to them, i.e. support staff need full information of the state of the enterprise, management need an abbreviated view of whether the enterprise is up, down, or indifferent!
Protects existing management infrastructure investment because all the work carried out so far on the management systems Netcool™/OMNIbus consolidates is not lost, the Netcool™/OMNIbus system adds value by making the information useful to everyone.

The point is, any organisation with a management platform, and multiple support people can use Netcool™/OMNIbus, from the correlation and automation, to the multi-user desktop environments.

6.2.2.1 Single Management Platform

Where an organisation you identify as a prospect has only one management platform, (i.e. SunNet Manager, HP-OpenView NNM, or IBM NetView for AIX) but they have multiple users wishing to view the manager at the same time, Netcool™/OMNIbus can help.

In the case of HP-OpenView NNM and NetView for AIX, the GUI topology map can be run several times from the same workstation and displayed using X windows to the client workstation. There are several problems with this:

- Extremely heavy load on main workstation processor which is also trying to do network manager
- No authentication of users using the management platform so that if only one person is authorised to use the CiscoWorks configuration tools for example, there are not restrictions, every user can access them, and in practice may be capable of doing damage to the network, although not maliciously
- Users cannot see the *real* state of devices, an icon flashing may mean that a single failure has occurred, or multiple failures there is no way of telling, *and* there is no way of acknowledging an alarm such that people know you

are working on it - in certain cases many people may end up working on the same fault concurrently.

With the installation of Netcool™/OMNIbus, apart from the benefits of fault consolidation (which with only one platform is not required) and correlation and automation (which will get used) the benefits to the user community are as follows:

- Reduced load on the management platform, since Netcool™/OMNIbus uses client server tools which can be run anywhere, and the Desktop can run on the workstation or PC that the user sits at.
- Multi-user Desktop tools (running on the personal workstation) with access security, allowing only those with sufficient authentication to run configuration tools etc.
- Real device state is now available to all users with a Desktop, and in addition, the information can be presented in different ways to specific users. Also, when alarms are acknowledged by a user, the other users are notified instantly by an update to the alarm display

In addition to the above, the Netcool™/OMNIbus system allows fault performance information to be automatically created to allow organisations to set realistic Service Level Agreement (SLA) documents based on the actual failure performance information of the enterprise - %Availability can be derived from the fault history information.

Netcool™/OMNIbus provides a significant level of added value to sites with only one management platform.

6.2.2.2 Multiple Management Platforms

Where multiple management platforms are employed in an organisation, all the value of the *Single Management Platform* approach apply here, but also some other benefits are obtained.

Some of the problems with a multiple management platform environment are detailed as follows:

- Different groups use isolated management platforms, although if the equipment they are managing fails, it may affect other objects in the network managed by a different group (and therefore a different management platform), leading to multiple people from different groups wasting time by investigating the problem
- Demarcation can become a problem in accounts with a very political structure - it's easy for one group to blame another because there is insufficient correlated information about the failures of items on the network.
- Fault relationships can be determined across the spectrum of managed objects, and inconsistencies can be monitored, i.e. if a particular application on the mainframe fails regularly, and after analysis of the Netcool™/OMNIbus data, it is noticed that something else on a, perhaps, completely unrelated piece of equipment fails, the relationship can be investigated and monitored. This is not possible without the consolidation of the management environment.

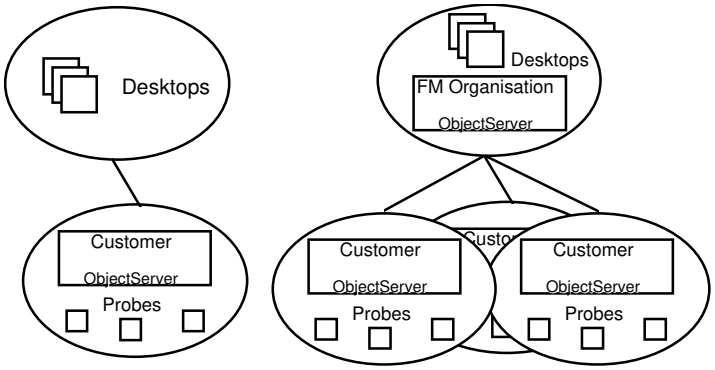
The Netcool™/OMNIbus system can consolidate all the management platforms in an enterprise (SNMP, Mainframe, Telephony, etc.), it can then provide correlation of faults across all the platforms which are consolidated, providing the users with accurate information as to the real state of the network, not just single point faults.

The phrase “Transforms fragmented ‘tactical’ domains into coherent ‘strategic’ management domains” says it all. Instead of working in isolation, and attempting to interpret the very limited information from their own single management platform, organisations can link all the management groups together to deliver a tightly coupled service working as a whole - the individual groups can still manage their own equipment in isolation, but will know when the failures in their domain have been caused by failures from another domain.

6.2.2.3 Remote Facilities Monitoring

Netcool™/OMNIbus is the ideal tool for those companies providing a remote facilities management service. Since the product is completely client server, both the Probes and ObjectServer could be run from the customer’s site, and just the Desktops used at the facilities management company, or, an ObjectServer/probe combination could be running at each customer, and another suite of ObjectServers at the monitoring company to link all the data together and then present this to users.

Again, because of the distributed nature of the product and the consolidation and correlation capabilities, the facilities management organisation will be able to provide a much greater level of management functionality than has been traditionally possible, *and* with the history/statistics information, accurately assess SLA figures.



Single Customer Multiple Customer Environment

The above diagrams illustrate how the Netcool™/OMNIbus system can be applied to facilities management environments.

6.2.2.4 Wide Area Monitoring

Where network management environments are spread over large areas, and an organisation is either forced to reduce the level of management performed (reduce polling intervals to remote devices because of the level of management traffic over the WAN), or implement a multiple management platform strategy, Netcool™/OMNIbus can help.

Effective management cannot be performed unless there is adequate information about the managed objects. If you are not collecting adequate levels of management information about a device then you might as well not bother to manage it.

To monitor remote sites effectively will require a multiple management system installation. Netcool™/OMNIbus Probes and ObjectServers can be implemented remotely, and the

management information can be consolidated at the central support site using another Netcool™/OMNIbus ObjectServer.

Note on Topology Maps: Organisations may (at first) say that they wish to continue to use, say HP-OpenView Node Manager's topology map as a user interface for their users. If they wish to do this, we can have this happen from the Netcool™/OMNIbus system by forwarding SNMP Traps to the OpenView NNM - users are not forced into using the Netcool™/OMNIbus ObjectiveView.

6.3 Netcool™/LegacyWatch

Netcool/LegacyWatch is a Client Server proxy agent system which allows any legacy/non-SNMP equipment to be managed by open management platforms such as SunNet Manager, HP OpenView, NetView for AIX and also integrate with Netcool™/OMNIbus

6.3.1 What is Netcool™/LegacyWatch

As Open Management Platforms such as SunNet Manager, HP OpenView Node Manager and NetView/6000 become the standards for managing open networks based on SNMP, it is necessary to integrate the management of older non-SNMP, and non-networked devices through these centralised platforms.

Netcool™/LegacyWatch is a client-server management system which provides a gateway from the old to the new, integrating any device or application which is manageable from a character terminal (or can send alerts to a printer port) to have its status and events integrated into the popular management systems.

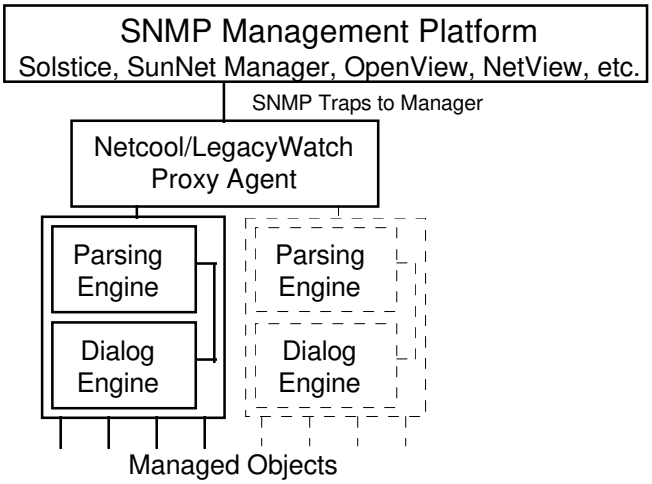
Netcool™/LegacyWatch makes a character stream connection to the target object, and scans the messages that the object generates, the resultant message can be modified or completely changed, then directed to the SNMP management platform as an SNMP Trap.

Netcool™/LegacyWatch can also periodically request information from the device to elicit messages. If a message matches an event condition, it is passed up to the management platform together with key information from the message. The manager (SunNet Manager, HP OpenView Node manager, NetView/6000) maps the event onto the icon which represents the object, and displays it as a change of state (or whatever condition the manager has set).

The event information can then be automatically passed to a fault management and trouble ticketing application.

Netcool™/LegacyWatch Features

- Integrates the management of your entire environment under one management platform umbrella
- Network Management: manage legacy networks of serial multiplexors, switches, PBXs etc.
- Device Management: manage devices which were previously unmanageable by open protocols or have no future open management direction.
- Console Management: monitor messages from computer consoles of an operating system such as AS/400, VAX VMS, and Mainframe systems, and generate fault alarms for any conditions. Connects via telnet, sethost, tn3270, RS232, 5250, etc.
- Entirely user configurable environment using a MOTIF GUI, including dialogues to elicit information, and pattern matching to detect events.
- Customisable "Event/TRAP" messages allowing real English fault messages rather than cryptic error codes.
- Managed Objects can be hosts, devices, process information or applications.
- Supports SunNet Manager, HP OpenView Node Manager, NetView/6000 and Netcool™/OMNIbus



The diagram above shows the component parts of the Netcool™/LegacyWatch system.

The Netcool™/LegacyWatch Proxy Agent is the interface between a Netcool™/LegacyWatch agent (combination of Dialog Engine and Parsing Engine) and the SNMP management platform. The Proxy Agent creates SNMP Traps from the information passed to it by the agent. The Proxy Agent is also referred to as the Netcool™/LegacyWatch ***Runtime***

The Netcool™/LegacyWatch Agent is a binary process developed using a graphical development tool. The agent is made up of two parts, the **Dialog Engine** and the **Parsing Engine**. Many Netcool™/LegacyWatch Agents can work with a single Netcool™/LegacyWatch Runtime Proxy Agent.

The Dialog Engine provides the interaction between the managed object and the system. The Dialog Engine allows a bi-directional command response conversation to be carried out between the agent and the managed object to enable the information of the alert to be obtained. Once the required alert or warning information has been obtained, this is passed to the Parsing Engine.

The Parsing Engine allows messages to either be restructured, or completely changed to a users requirements (so that meaningless messages can be replaced by English for operators to comprehend, then this message is presented as an SNMP Trap to the management platform.

Note: Netcool™/LegacyWatch does not have a MIB, so the management platform cannot request ad hoc queries for information from the managed object, although the user of the management platform can run the Netcool™/LegacyWatch Agent to produce a status check.

Netcool™/LegacyWatch is a system which will be of use to any organisation running an SNMP management platform such as SunNet Manager, HP-OpenView NNM, or IBM NetView for AIX who want to integrate some telephony, or console environment into the SNMP manager, but are not looking to build a strategic management environment - should they require a strategic management environment, then Netcool™/OMNIbus is the choice.

Some of the more common uses for the system are:

- integrating the important console messages from legacy computer equipment such as DEC VAX, IBM AS/400 and IBM ES/9000 type

mainframes. Netcool™/LegacyWatch simply logs into the system and monitors the console logs, if certain messages i.e. DISKFULL, etc. are registered, then the user of the SNMP management platform can be alerted via a flashing icon of the device on his topology map.

- alert messages from telephone switching systems (PABX, ACD, MUXs, etc.) and changing the message from a meaningless string of numbers to a message in English detailing the failure. The importance of Netcool™/LegacyWatch here is that the telephony equipment produces so many messages that it is easy to miss important ones - now they can be isolated automatically reducing the possibilities of human error.

What the user will see is an icon for the device in his topology map (on the management system) and whenever it changes colour, he can look at the manager's event/trap log and see what fault has occurred.

6.4 Netcool™/Messenger

The Netcool™ products are designed to provide management integration where either products exist, but do not address the issues of real users, or where there are no product offerings and there is a critical user requirement.

Netcool™/Messenger is a product module specifically for the Netcool™/OMNIbus system. The product integrates voice and telephony with Netcool™/OMNIbus to provide remote control and notification services via standard telephone lines.

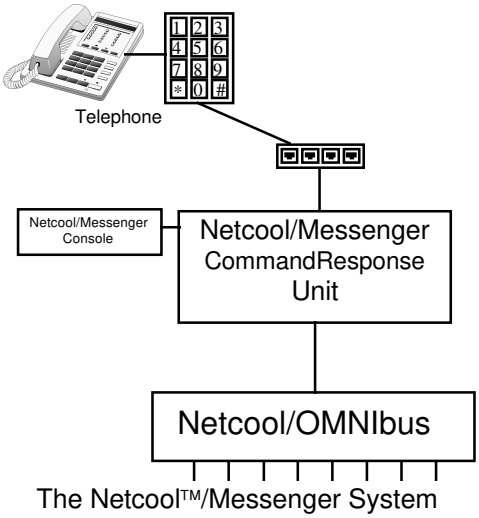
6.4.1 What is Netcool™/Messenger?

Netcool™/Messenger is an integrated voice system for the Netcool™/OMNIbus system. The product allows users of Netcool™/OMNIbus to be in touch with the state of the managed networks from anywhere in the world that has a telephone system (capable of connecting to the location of their Netcool™/OMNIbus system).

Netcool™/Messenger can call people on nominated telephone numbers, when the user answers, they are prompted with a voice warning that this is Netcool™/OMNIbus calling (or whatever they want it to say) and to enter their PIN number on the telephone keypad.

Once the user has entered his or her PIN code, the system “reads” the important alerts to them. They can then take actions at the Netcool™/OMNIbus server from a menu of items (based on their user level), using the telephone keypad.

Netcool™/Messenger is a hardware and software solution, requiring an Intel® type personal computer and telephone line hardware (all supplied) with the associated Microsoft Windows, TCP/IP and X Windows based administration tools.



The Netcool™/Messenger System

Netcool™/Messenger adds a level of support above that provided by traditional network management and fault automation systems, and is completely configurable by the systems administrator of the Netcool™/OMNIbus system.

7. Case Studies

7.1 A Telecomms Carrier Monitoring Its Data Network Infrastructure

A large international telecomms organisation with an extensive datacomms internetwork. The internetwork includes Hubs, Routers, Hosts, and legacy Mux, connectivity and telephony equipment.

Initially the organisation was supporting over 20 management platforms (element and heterogeneous) for the environment, not to mention scores of character terminals giving dumb scrolling information from legacy equipment.

The scale of the enterprise has to be seen, but the following bullets describe the environment

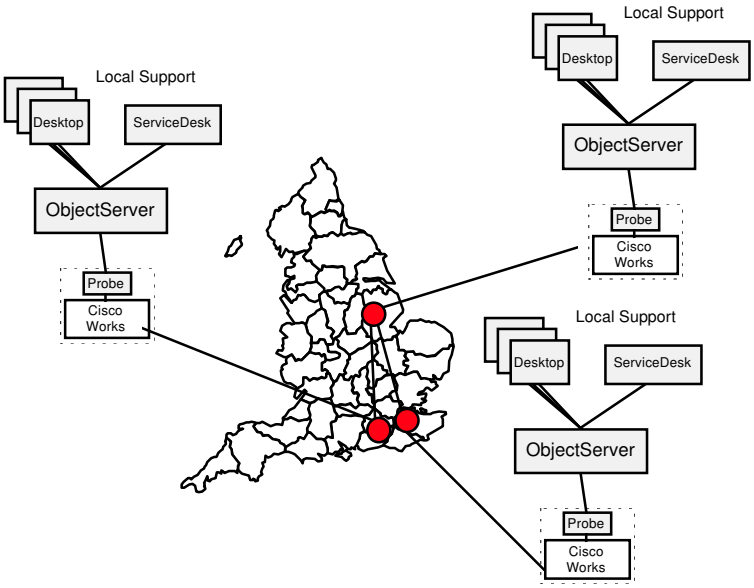
- 250,000 managed entities
- 2 management centers, 1 disaster recovery site
- 2,500 Cisco Routers
- 2,500 ACC Routers
- 3,000 Bay Networks and other HUBs
- n000's Unix Servers
- 40,000 legacy Mux, TDM, PBX, switches
- n00's Ascom TimePlex Routers and Muxes
- n00's Stratacom Frame Relay Switches
- DEC VAX hosts

The network has over 250,000 devices which require management.

An operational problem for the organisation is that it has a number of support centres located around the UK, all supposed to be working co-operatively, but in practice, working in isolation.

They needed to group-up, consolidate information, correlate on a large scale, and define a Virtual Private Network views which map to customer SLA, and then use a Service Level Management system to monitor this real-time.

Following is a simplistic illustration of the solution.



To address the problem, the organisation implemented a combination of Micromuse Netcool™ products.

Netcool™/LegacyWatch was implemented to pro-actively monitor all the existing legacy managed elements into a consistent environment. This required complex dialogs between the legacy Mux, PBX and switch equipment. There are 40,000 devices in all.

The Netcool™/OMNIbus system has then been implemented with ObjectServers in each support centre, having Probes into the various management platforms implemented

- SunNet Manager for Cisco Routers
- HP-OpenView Node Manager for Hubs and LAN Probes & ACC routers
- NetView for AIX for Unix management
- DEC PolyCenter CM for DEC equipment
- DECmcc
- Timeplex TimeView 2000 for Ascom Timeplex equipment
- StrataView+ for Stratacom equipment
- Netcool™/LegacyWatch for non-SNMP equipment

Now, a consistent view of the entire network (showing correlated relationships) is available for every authenticated support person in any support centre.

The entire environment can be administered from a single view (again if the user is authenticated), and the group can provide fault statistics for any managed element in the environment.

An example of some of the benefits to the organisation are:

1. On average, the group were receiving ~75,000 alarms per day - Netcool™/OMNIbus automatically de-duplicated the alarm stream down to ~150/200 alarms per day.
2. There are two actve support centers, there was no way of co-ordinating the management between them. Netcool™/OMNIbus solves this.
3. There are several layers and skill levels of support staff, Netcool™/OMNIbus provides authenticated access to applications, and graphical views tailored to suite the level of operator.

The Netcool™ products have improved the way of life for the operators and back en support people simultaneously, and in addition has allowed management to have a view into the performance of the network both on paper and real time.

Most importantly, the system has been implemented in a very short time, with the minimum of consultancy required. The support personnel have been able to implement all correlation and automation themselves using the GUI of the Netcool™/OMNIbus system.

7.2 A High Street Financial Organisation Monitoring Burglar Alarm Systems

A high street Building Society with over 200 branches is increasingly becoming the victim of organised crime, having its own an other building societies in a particular town systematically and concurrently burgled on a particular night.

The problem is so bad, that local Police forces do not have the manpower to control the situation.

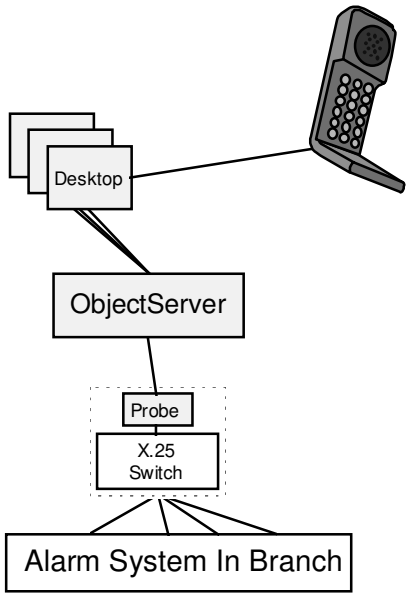
When the Society is burgled, the offending burglar severs various telephone, modem, fax and ISDN equipment to disable the alarm system.

The Netcool™/OMNIbus system in conjunction with a Netcool™/LegacyWatch Agent, detects that certain conditions have occurred simultaneously, then carries out further proactive detection routines.

Once Netcool™/OMNIbus has satisfied it's rules conditions, a fax is sent to the Building Society's Security Dispatch centre, where the local duty security manager calls the Police station closest to the branch office being burgled.

The system paid for itself when it detected it's first burglary, it has been 100% successful, and has also detected a fire in a branch.

The alternative to the Netcool™/OMNIbus solution was a system costing almost £500,000.00 rental per annum. Or, rely on the Police, and luck.



7.3 A Telecomms Company Providing Customer Network Management

A major telecommunications organisation have developed a facilities management group, whose objective is to manage end user customers networks (outsourced from the customer).

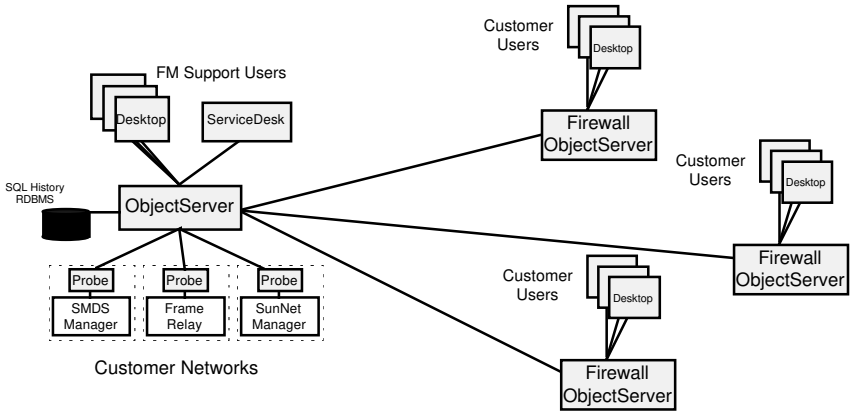
The environments being managed include all SNMP equipment for interconnected LANs and WANs. The brief of the organisation is to monitor the customer networks, identify failures, and fix them to certain predefined Service Level Agreements (SLAs).

Should the supported infrastructure have a fault which takes them outside the SLA figure, then the FM group start to owe the customer money!

The problem for the Facilities Management group was that, although there are many off the shelf SNMP management platforms, whether they chose all from the same brand, or many different brands, they has no way of linking them together. In addition, with all the support people they had (some specialists, and others more front end operators, there was no security authentication control, or a way of having a single view into the network).

Another aspect of the scenario is that many customers wished to have a view into the management being performed on their network. The problem here is that the FM group were (in certain cases) using a single management platform to monitor many different customers, and this made it very difficult to provide a view for the customer.

The organisation chose the Netcool™/OMNIbus system to bridge the gap in the functionality provided by the “standard” SNMP management platforms to give a truly integrated management environment.



As you can see from the diagram above, many customer networks are managed by many SNMP management platforms (of various kinds).

The Support personnel in the FM group have a view into the networks being managed, and keep a database of fault histories (allowing them to produce reports of aspects of availability.

For the FM group management team, different levels of support personnel have a different (but consistent) view of the enterprise, and where faults that they see are related to other faults managed by another group, correlation is done to show critical and non-critical faults to that group or individual.

FireWall ObjectServers are used to provide a view to the customer of the management being performed on their network, with all the filtering being performed at the master ObjectServer.

The FM group's support personnel do not use the SNMP management platform console, all access to management platform tools, partner applications, and proactive activities is performed using the Netcool™/OMNIbus Desktop.

8. Competition and Other Noise

Netcool™/OMNIbus is the only Service Level Management system for Virtual Private Networks which is available, although some of the facilities provided by the Netcool™ products place us in the category of “Manager of Manager” (MoM) type systems.

As discussed in the notes for section 2.0, the Netcool™ products do not constitute a MoM as we would describe one, but since we are categorised as this, and have similar functionality to other products describes as MoMs, then we should make comparisons of our own product to those of our competitors.

Incidentally, Netcool™/OMNIbus could be described as a Monitor of Managers though, since we are non-intrusive to the management platform but do utilise all fault information from the management platform.

The competition in the MoM market is fairly limited. There are really only two companies, MAXM Systems, Inc. with a product called *MAXM*, and Boole and Babbage, Inc. with a product called Command/Post.

We have included two other products in the competition profiles though, OSI-NetExpert from Objective Systems Integrators, Inc. because although it does not fit in the MoM space, it is both competitive in certain functionality items and markets, and OSI-NetExpert has an interesting background along with MAXM and Command/Post.

8.1 History of the MoM

A little history, once upon a time there was a small US based start-up called AvantGarde, Inc. AvantGarde had an idea - to produce an alert consolidation system for IBM Mainframe Datacenter departments which would allow many operators to view the state of all the aspects of the systems from their own desktop computer.

AvantGarde made a small, incy wincy mistake in their product design. The product (called Net/Alert) was developed for IBM mainframe operations departments, and therefore to be sold into the domain of the IBM salesman. Unfortunately the major mistake that AvantGarde made was to develop the Net/Alert on Sun workstations, for implementation on Sun workstations.

Therefore to implement AvantGarde’s Net/Alert system, each Net/Command system user would either have had to have a Sun workstation on their desk, or replace the IBM 3270 type terminal they were using with a PC equipped with both TCP/IP and X Windows, and the IBM SNA communications packages - which at that time would require an extremely expensive PC and be difficult to set up.

Consequently, AvantGarde (who were fairly ahead of their time with the product) went bottoms up (or Chapter 11) in the US, and looked around for a buyer.

An organisation called Objective Systems Integrators, Inc. looked over the company, and made noises about buying AvantGarde. Unfortunately, they decided not to buy AvantGarde, but to create a new product that (incredibly) had a similar architecture to the AvantGarde Net/Alert product. The product they developed is now called OSI-NetExpert which, the company targeted at the management requirements of telecomms companies.

Next, an organisation called ITM, Inc. investigated the purchase of AvantGarde. Like Objective Systems Integrators, they looked at the company, evaluated the architecture of the product in detail, then decided to develop their own product. The product they developed they called MAXM (later changing the company name to MAXM Systems, Inc.) and aimed the product squarely at the IBM Datacenter alert consolidation market place. Unlike AvantGarde though, MAXM was developed on IBM hardware, making it attractive to IBM Datacenter people.

Finally, after much positioning, a company called Boole and Babbage (a mainframe based software vendor) purchased AvantGarde and therefore the Net/Alert product, and changed its name to firstly to Net/Command, and then later to Command/Post.

So, although the three products look very different in terms of hardware and implementation, they are all based on the original technology (early 1980's) of AvantGarde's Net/Alert.

The following discusses the offerings from these vendors, what they are sold as, and their deficiencies to the Netcool™ range of products.

8.2 MAXM Systems, Inc. MAXM

8.2.1 Overview

MAXM, from MAXM Systems, Inc. is an alarm consolidation and automation development system that consolidates and filters events from legacy equipment (and SNMP managers according to MAXM themselves!). The product has been designed specifically to work in the IBM SNA and mainframe environment and to appeal to IBM Datacenter departments. MAXM does not do correlation, although, hardwired rules can be created with complex, bespoke development.

8.2.2 Technical Description

The system uses a Unix server (RS/6000 running AIX) to collect it's data from the fault feeds (IBM mainframe consoles and other applications) and that information is passed on to user desktops running OS/2.

Communication between the server (on AIX) and the clients (on OS/2) uses IBM's APPN LU6.2 protocol (whereas Netcool™/OMNIbus uses Sybase OpenServer technology). APPN means that MAXM are completely locked in to a proprietary communications architecture - it is extremely difficult for them to move into open systems (TCP/IP) without a complete re-architection of their product.

Unlike Netcool™/OMNIbus, where all processing is done at the ObjectServer, thus enabling the Desktop tools to run on un-complex operating systems (Microsoft Windows, etc.) MAXM relies heavily on the ability to perform complex processing at the user Desktop, so they *have* to use OS/2 on the desktop because of it's multi-tasking capabilities. Users have been asking MAXM for years to do a Windows interface, but they are always told "it's coming..." - THEY CANNOT DO IT WITHOUT DRASTIC RE-ENGINEERING!

8.2.3 Competitive Profile

There is a fundamental difference between Netcool™/OMNIbus (and the other Netcool™ products), and MAXM (in fact and Command/Post and NetExpert).

Netcool™/OMNIbus is a configurable application, whereas MAXM is a development toolkit.

Configurable applications can be installed and operational immediately, then configured using the graphical tools to perform other functions - such as correlation.

Configurable applications, by their nature are easily and cost effectively supportable.

Development systems (MAXM, Command/Post, NetExpert) require considerable amounts of consultancy after installation, and therefore do not become operational for many months.

Micromuse has modularised the Netcool™ product range.

Netcool™/OMNIbus a Service Level Management system with authenticated multi-user Desktops, shrink wrapped Probes (using the Netcool™/OMNIbus API) to management platforms, and the core ObjectServer being automatic, and distributed.

Netcool™/LegacyWatch allows non-standard management platforms, and ASCII feeds to be monitored and linked into Netcool™/OMNIbus.

MAXM have only one product with no shrink wrap capability, a reliance on proprietary networking (LU6.2 APPN), and operating systems OS/2.

MAXM claims to have an interface to IBM's NetView for AIX. As far as we can tell, this interface is not shrink wrapped like one of the Netcool™/OMNIbus Probes (meaning that MAXM has no API to their system) - it is also rumoured that this interface does not exist, since they are no longer included in the NetView Association documentation.

Each time MAXM wish to sell a NetView for AIX connection to MAXM, they have to develop it - this is because the only way they can monitor events from *any* device is by developing a Netcool™/LegacyWatch type interface.

There is no API to MAXM. Translated into English, this means that for MAXM to implement a solution, it takes *a very long time, and is bespoke for each customer*

MAXM's automation rules are very complex to set up and the system does NOT DO CORRELATION (although hard coded rules can be programmed - normally by MAXM consultants.

Netcool™/OMNIbus automation is performed using SQL, and works very efficiently since it is direct on the database. Of course we have a fairly sophisticated drag and drop GUI automation builder for correlation and automation, which means NO SCRIPTING!!!

MAXM has to use a language similar to a proprietary IBM mainframe scripting language called REXX (sounds like a dinosaur doesn't it?). This REXX-like language requires an experienced operator to make sense of, and is not very efficient in the way it works with the data on the MAXM system, making it difficult to develop, complex to implement, and slow to use.

8.2.4 MAXM in Summary

In short, MAXM does not support shrink wrapped installation, cannot provide correlation, cannot integrate the SNMP management platforms (without oodles of custom development), requires a complex C like scripting language to develop any automation (which can take a long time), and requires proprietary operating systems and communications software.

The MAXM desktop environment is graphical (event list and topology map), and does support multi-user/security authentication. The desktop tools though do not support context specific *tools* menu's from the event list or topology maps - do not underestimate how powerful this capability in Netcool™/OMNIbus actually is!

Micromuse's Netcool™/OMNIbus is the world leader in the Service Level Management of Virtual Private Networks. Netcool™/OMNIbus is a configurable application, rich in features that comparable products cannot match. Having said this:

- MAXM are a major player in the automation market
- MAXM sales strategy which is particularly aggressive, and sometimes "dirty" against the Netcool™ product range
- MAXM have a marketing/reseller agreement with AT&T GIS to provide MAXM (called MAX/Enterprise) for their OneVision management architecture (similar to Complexity Management) on top of HP-OpenView
- As Netcool™ sites become more mature we will encroach on the mainframe automation space and thus MAXM's core market - so don't expect the "selling" part against MAXM people to become easier.
- MAXM ***does not*** allow Service Level Management, or the mapping of Virtual Private Networks
- It's funny, but MAXM sales people now talk about "Probes" - wonder where they got that idea from...particularly as we always explain that they are not Probes...!!!

8.2.5 MAXM Pricing

The MAXM product starts with a retail price of around £150,000.00 for a "simple" system, and with basic consultancy offerings (which people *will* require to do anything useful with the product) the price rises to more than £250,000.00.

8.3 Boole and Babbage, Inc. Command/Post

The Command/Post system (due to it's ancestry) is very similar in architecture to that of MAXM, except that Command/Post runs on Sun hardware using SunOS, and has an X Windows system client for SunOS.

Command/Post, just like MAXM is mainly aimed at automating the mainframe environment. Begrudgingly Command/Post now supports the inclusion of alerts from SunNet Manager, HP-OpenView NNM, and NetView for AIX (they say), but does not support any of the other management platforms that Netcool™/OMNIbus supports with our shrink wrapped Probes.

Command/Post has no API to it's database (similar to MAXM), so to "connect" to the event sources that the system monitors and does not do correlation, a custom developed Netcool™/LegacyWatch style agent has to be developed (which is a binary application).

The difference between a Netcool™/LegacyWatch agent, and the Command/Post agent is that the Command/Post agent does not support “polling”. This means that it has to rely on event information coming into it, rather than initiating a dialogue with the managed object.

For example, dialogue allows Netcool™/LegacyWatch to have a conversation with a device to get the information it requires so if several commands and responses have to be run on the target system being managed

The Netcool™/LegacyWatch Dialog Engine can do this and then send the information on to the Parsing Engine, where the information is translated into a usable message.

Command/Post can only listen for faults, it does not support the notion of dialogues or command/response - this means, to a user, that it either may not be capable of getting certain information in the first place, or, that the system cannot do any low level filtering, where most of the information coming from the managed object is noise.

Command/Post retail pricing starts at around £100,000.00, but there are significant levels of consultancy required to implement the system which can take a simple installation well over the £250,000.00 mark and more.

8.4 Objective Systems Integrators, Inc. OSI-NetExpert

Objective Systems Integrators chose to take a different path with their implementation of the AvantGarde Net/Command system. Instead of following the trend and providing event management and automation for mainframe environments, OSI have developed OSI-NetExpert into a telecomms management platform.

OSI-NetExpert has evolved into a telecomms network management platform. The product supports the management of SNMP, and OSI network management based agents using proxy agents, and has a Netcool™/LegacyWatch type system which allows for the management of non-intelligent devices.

In the US, OSI-NetExpert is well deployed in telecomms companies with over 40 sales of the individual product, although it is unknown how many actual companies this translates to, OR IF THEY HAVE EVER GOT THE PRODUCT WORKING!

Netcool™/OMNIbus in theory should not compete head-to-head with OSI-NetExpert, since we consolidate faults from multiple management platforms and legacy equipment, then correlate and automate the information, and OSI-NetExpert is a management platform in it’s own right. (In fact, Netcool™/OMNIbus can integrate OSI-NetExpert into its framework with a Probe for the product).

In practice, OSI-NetExpert is direct competition in the telco space. This is because most sites that need an integrated telecomms management platform actually need the Netcool™/OMNIbus and Netcool™/LegacyWatch combination to link in multiple management platforms and non-intelligent equipment together under a single framework. OSI-NetExpert is sold into sites to perform this role, and consequently requires many hundreds of hours consultancy to provide what is essentially a bespoke and proprietary system to the customer.

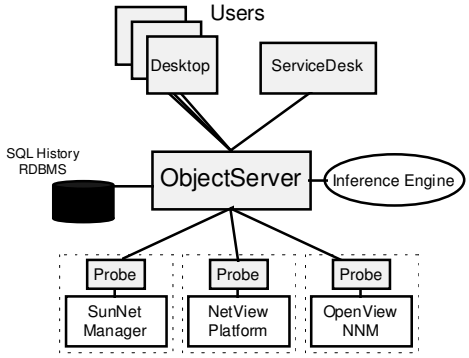
OSI-NetExpert does have an interesting piece of functionality not found in the other systems discussed here, it has an Inferencing Engine (providing a level of artificial

intelligence). The Inferencing Engine works at OSI-NetExpert's equivalent to Netcool™/LegacyWatch, to perform automated activities based on its own experience of previous faults/events.

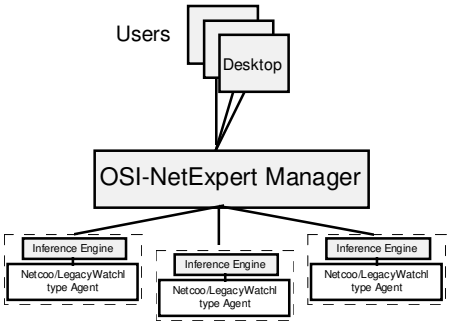
Micromuse have the inferencing capability in Netcool™/OMNIbus version 3.0, but there are some differences to the Netcool™/Decision (not announced name) module's functionality in the Netcool™/OMNIbus architecture, and the way it is implemented in OSI-NetExpert.

Netcool™/OMNIbus's Inferencing system works at the ObjectServer layer, meaning that intelligent decisions are made by the inferencing engine based on *all* information available from *all* the management platforms and legacy systems being monitored.

ISO-NetExpert's inferencing however, works at the Netcool™/LegacyWatch layer, meaning that it can only perform inferencing on data from a single point, not from the whole environment as with Netcool™/OMNIbus. In addition, because the inferencing requires so much processing power. OSI-NetExpert suffers from severe performance limitations with respect to the number of alerts per second it can process.



The Netcool™/Decision approach



Inferencing with OSI-NetExpert

The above diagrams clearly illustrate the differences in architectural approach to between Netcool™/OMNIbus and OSI-NetExpert to providing the artificial intelligence inferencing capabilities. The OSI-NetExpert system cannot provide inferencing using all the information available from the platform.

OSI-NetExpert has a retail price of around the £250,000.00 mark, but with the consultancy required to make the system perform any useful functionality, the price approaches £500,000.00 and more...If you are ever in a competitive situation with the OSI-NetExpert system, just encourage the customer to evaluate both, OSI does not evaluate well, the OSI-NetExpert sales person always sells by installed base reference, rather than showing the customer what the system will do on their site...simply because too much work is required to get the system running.

8.5 Competitive Feature Breakdown Matrix

↓ *Feature* *Product* →	Netcool™	MAXM	OSI-NetExpert	Command/Post
Alarm Consolidation	Yes	Yes	Yes	Yes
Multiple Alarm Sources	Yes	Yes	Yes	Yes
Integrates Standard SNMP Managers	Yes	No	No	No
Multi-platform "drag & drop" Correlation	Yes	No	Yes	No
Management of Virtual Private Networks	Yes	No	No	No
GUI Administration of Automation	Yes	No	No	No
Programmer APIs (C & SQL available)	Yes	No	No	No
Operational in *Days* rather than *Months*	Yes	No	No	No
User Security Authentication	Yes	Yes	Yes	Yes
Multiple Consolidated Topology Maps	Yes	Yes	Yes	Yes
Multiple Filtered Event Lists	Yes	Yes	Yes	Yes
Context Specific "Tools" Menus	Yes	No	Yes	No
Automatic De-duplication of Events	Yes	No	No	No
X Windows Desktop Environment	Yes	No *OS/2	Yes	Yes
Exclusive Management Paradigm	Yes	No	No	No
Scaleable Distributed Architecture	Yes	No	No	No
Integration to Standard Helpdesk Products	Yes	No	No	Yes
Voice Telephony Alert Management Integration	Yes	Yes	No	Yes
Client Server, Configurable Application	Yes	No	No	No
Uptime/Downtime, and %Availability History DB	Yes	No	No	No