State of Art Survey: Intra-domain and Inter-domain Management of Smart Space Environments

Robert O'Connor,
Telecommunications Software Systems Group,
Waterford Institute of Technology.

Abstract
This paper surveys network management architectures and their applicability to Smart Space environments. It highlights lessons that can be learned from SNMP, X.700, TMN and CIM with respect to developing a multi-domain Smart Space architecture based on the following criteria: architectural information components; communications protocols and formats; management services.

Keywords Ubiquitous computing; Pervasive computing; Smart Spaces; Network Management; Intra-Domain; Inter-Domain; TMN; SNMP; OSI X.700; CIM; Management of Smart Space Environments.

1. Introduction

Ubiquitous Computing; Pervasive Computing; Smart Spaces – these are all terms used to describe the strongly emerging trend in Information Technology towards highly dynamic, heterogeneous, computing environments. Areas utilising ubiquitous technology usually exhibit the following characteristics:

- contain numerous, casually accessible and often invisible computing devices
- utilise mobile and imbedded environmental infrastructure
- connect to an increasingly ubiquitous network structure

The basic definition of a Smart Space is a physical space rich in devices and software services that is capable of interacting with Users, the physical environment and external networked services. As computing power increases, hardware size decreases and programming techniques become more accessible, the potential for mobile computing is growing. Within Smart Spaces everything has the possibility of being a computer. Pervasive Computing is about creating such technologies and infrastructures and developing the devices and services that will deliver this ubiquitous computing experience.

The research topic, "Intra-domain and Inter-domain Management of Smart Space Environments" has the potential to yield many benefits that could contribute greatly to the field of Ubiquitous Computing. There are many projects across the globe engaging in research into certain specialised areas of Smart Space technology. However, very little effort is being expended on the management structures that will allow differing component technologies to successfully inter-operate with one another. Intra-domain management is concerned with the internal management of a Smart Space, while Inter-domain management is concerned with external communications and operability across multiple Smart Spaces.

This paper summarises computer network management architectures and the more traditional telecommunications network management techniques and highlight aspects of these architectures that may prove useful when attempting to describe future network architectures for emerging ubiquitous environments. The successful deployment of truly ubiquitous services is dependent on these heterogeneous Smart Space environments communicating, collaborating and interacting with one another, hence it is vital that intra and inter zone architectures are studied, researched and developed.

This paper has the following structure: Firstly, network management architectures that are of interest to the M-Zones project are given a brief overview. Then, each architecture is analysed based on the following criteria: architectural information components; communications protocols and formats; and the services each management structure provides. After this, the management architectures are discussed in terms of the direct relevance each bears to the M-Zones project. Research projects with similar goals to M-Zones are also identified and briefly evaluated in this section. Finally, conclusions are drawn and future work outlined.

2. Overview

The Simple Network Management Protocol (SNMP) (Case, Fedor, Schoffstall & Davin, 1990) was originally designed for the management of networks based on Internet Protocols (IP). The basic principle of SNMP is simplicity (KISS - keep it small and simple). This results in small, simple, and mostly cheap Agent software applicable for the devices of IP-based networks, such as modems, bridges, hubs, routers, printers, etc. SNMP defines a framework for the management of IP based data communication network devices. With the different versions of SNMP (v1, v2, v3), the functions added have become increasingly more complex. SNMPv3 resolved this problem by using modularity to allow the evolution of portions of SNMP without requiring a redesign of the general architecture.
The goals of SNMP are:

- the complexity and number of management functions in the management agent should be kept to a minimum (i.e. keep the agent as light as possible)
- the functional paradigm for network control and monitoring should be sufficiently flexible and extensible to accommodate unanticipated additional network functions
- the management architecture should be independent of the architecture of the gateway or hosts

The X.700 OSI Management Environment (ITUT-X700, 1992) includes both the capability for managers to gather information and to exercise control, and the capability to maintain an awareness of and report on the status of resources in the managed network environment. This responsibility may be manifested in terms of autonomous management of the open system and co-operation with other open systems; through the exchange of information; and through the performance of co-ordinated management activities. Systems management provides mechanisms for the monitoring, control and co-ordination of resources and protocol standards for communicating information relevant to those resources. In order to describe management operation on resources, resources are viewed as managed objects with defined properties. Information required for systems management purposes in any open system may be provided through local input; may result from input from other open systems through systems management communication; or may be a result of lower layer network protocol (Zimmermann, H, 1980) exchanges.

Telecommunications Management Network (TMN) (ITUT-M3000, 2000) provides an architecture to transport, store and process information used to support the management of telecommunications networks and services. It is based on the X.700 OSI Network Management Model as described earlier.

It also employs other OSI application service frameworks such as X.500 Directory Service (ITUT-X500, 1993), but these are beyond the scope of this document.

The Distributed Management Task Force (DMTF) is an industry association dedicated to promoting and developing standards for distributed environments, systems management and interoperability. The Common Information Model (CIM) (DMTFa, 1999) is an object-oriented information model that provides a framework through which management data can be abstractly modelled.

3. Analysis

The management architectures are now discussed in terms of architectural information components; communications protocols and formats; and the services that each provides.

3.1 Information Architecture Components

3.1.1 SNMP

With SNMP, the guiding principle is simplicity. Management information is stored in a Management Information Base (MIB) in the form of Managed Objects (MO). An SNMP MO is not an object in the object-oriented sense, but instead represents a variable object. Instances of MOs can be accessed with the protocol elements of SNMP to traverse tables and to send simple traps (messages) to notify managers about events that have occurred at the controlled devices. Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, which have management agents responsible for performing the network management functions requested by the network management stations. SNMP is used to communicate management information between the network management stations and the agents in the network elements.
(Case, Fedor, Schoffstall & Davin, 1990)

3.1.2 OSI

Management of a communications environment is an information processing application. Because the environment being managed is distributed, the individual components of the management activities are themselves distributed. Management applications perform the management activities in a distributed manner by establishing associations between systems management application entities.
(ITUT-X700, 1992)

An MO is the OSI Management view of a resource that is subject to management, such as a layer entity, a connection, a Directory Service Agent or an item of physical communications equipment. Thus, an MO is the abstraction of such a resource that represents its properties as seen by and for the purposes of management. An essential part of the definition of an MO is the relationship between these properties and the operational behaviour of the resource. This relationship is not modelled in a general way.

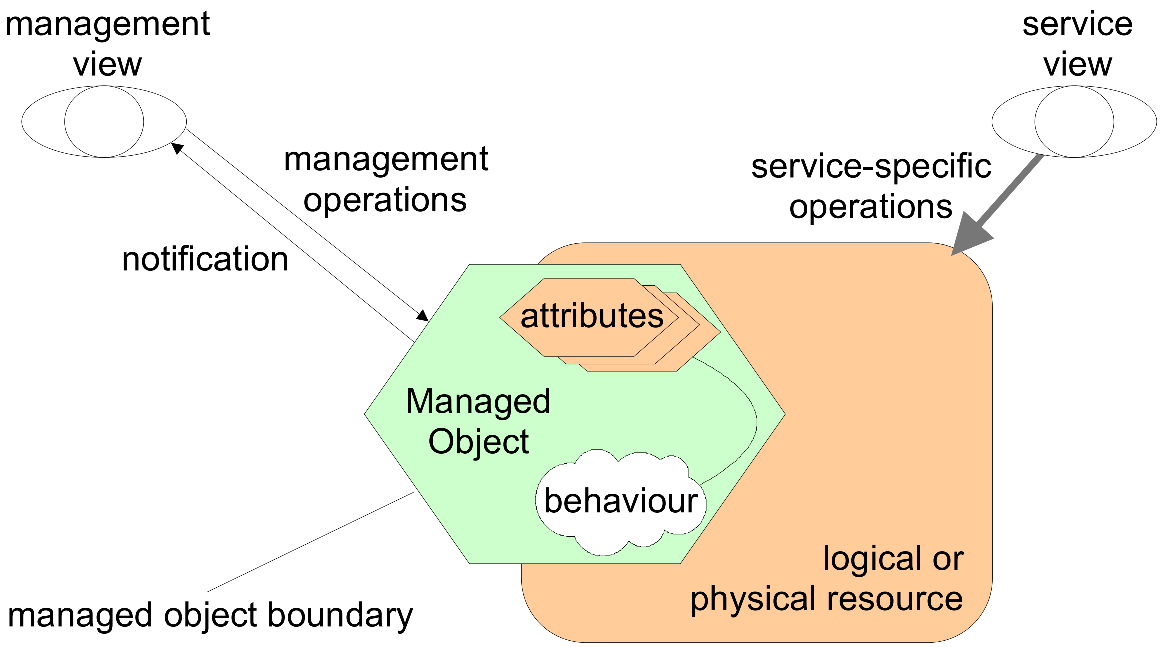

Fig 3.1.2.1 Managed Object

Managed Objects can be specific to an individual layer of the OSI Network Model (ITUT-X200, 1994), in which case they are known as (N)-Layer MOs. MOs that are relevant to more than one layer, to a specific systems management function (management support object) or to the system as a whole are known as Systems Managed Objects.

The distinction between the MO as visible to management and the resource that it represents may be described by saying that the attributes, operations and notifications are visible to management as the Managed Object Boundary, whereas the internal functions of the resource are otherwise hidden from management. The concept of a managed object boundary is an abstract idea and may have no implications during implementation.
(Zimmermann, H, 1980) (ITUT-X720, 1992)

A Managed Object class is defined as a collection of packages, which are comprised of:

- The **attributes** visible at the MO's boundary
- The **operations** that can be applied to the MO
- The **behaviour** exhibited by the MO
- The **notifications** that can be emitted by the MO

An MO is an instance of an MO class. An MO exists (from a management perspective) if it has a qualified name and supports the operations and notifications defined for its class. Objects may logically exist that possess MO class properties, however unless they obey the above criteria, they do not exist from a management point of view. MO classes are arranged in a class hierarchical structure of superclasses and subclasses. This structure obeys logical inheritance laws whereby subclasses inherit all characteristics of their superclass. The OSI model also supports multiple inheritance, where MO classes may directly inherit from more than one superclass.
(ITUT-X720, 1992)

A group of Managed Objects that are comprised in a distributed system is said to be a Management Information Block (MIB). The programs that perform management operations on these MIBs are known as Management Information Services (MIS). An MIS program taking on the role of an Agent is the part of a distributed application that manages the MOs in its local environment. An Agent performs management operations on MOs as it is instructed from the Manager. An Agent will also forward notifications from MOs to the Manager.

An MIS program taking the role of a Manager is the part of a distributed application which has responsibility for one or more management activities. The Manager issues operations and receives notifications from Agents. An MIS program taking the role of Manager is not limited to applications engaging solely in systems management; other application requiring access to management information may take on this role.

Roles are not permanently assigned to MIS-programs. Some MIS programs can be restricted to taking on only an Agent role or only a Manager role, while others can take the Agent role in one interaction and the Manager role in another.
(ITUT-X700, 1992)

3.1.3 TMN

TMN management is performed through the use of Operations Systems (OS). A TMN provides management functions and communications between interconnected OSs and between OSs and the various parts of the telecommunications network. A TMN may also provide management functions and communications to other TMNs or TMN-like entities in order to fully support the management of wide range of telecommunications networks. A telecommunications network consists of many types of analogue and digital telecommunications devices and associated support equipment. When network management is applied, these devices are generically referred to as Network Elements (NEs). A TMN-like network is a network that is not based on the TMN model, but can interwork and communicate with a TMN.

A TMN is conceptually a separate network that interfaces with a telecommunications network at several different points to exchange information and to control its operations. A TMN may also use parts of the telecommunications network to provide its own communications and thus, there is a requirement for a certain amount of self-management to be performed on a TMN.

The **Information Architecture** describes the nature of information that needs to be exchanged between the functional building blocks of a TMN. Management of a telecommunications environment is an information processing application. Because such environments are distributed, the network management is also a distributed application. This involves the exchange of management information between management processes to monitor and control various physical and logical network resources. The management information is considered from two perspectives:

- The **Management Information Model** is an abstraction of management aspects of network resources and related supporting activities. This model determines the scope of the information that may be exchanged, concentrated at the application level and involves a variety of management application functions such as storing, retrieving and processing information. These functions are referred to as "TMN Function Blocks".
- The **Management Information Exchange** concerns itself with lower levels of the OSI network layer model (Zimmermann, H, 1980) such as the communications layer and provides

functionality that allows physical components to attach themselves to the telecommunications network.

Because TMN is based on the X.700 model, a similar architecture comprised of Managers, Agents and Managed Objects is observed. Depending on the management function being performed at the time, management entities can take on either the Manager or Agent role. When a component assumes the Manager role, it takes responsibility for issuing management operation directives and receiving notifications. A component in the Agent role directly manages the associated Managed Object (MO) and receives and responds to directives issued by a Manager. It will also reflect a view of these MOs to a Manager and emit notifications concerning their behaviour.

Typically, “many-to-many” (M-N) relationships will exist between Managers and Agents in the sense that one Manger may be involved in information exchanges with several Agents, and one Agent may be involved in information exchanges with many Managers.

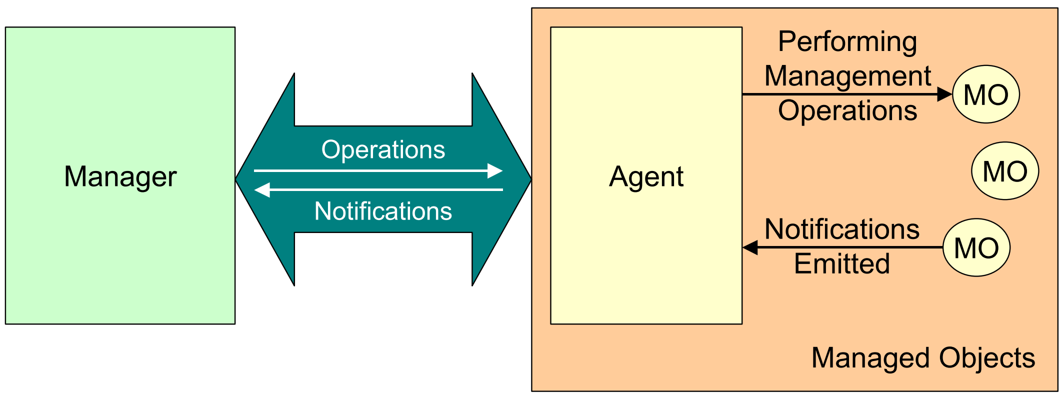

Fig 3.1.3.1 Information Architecture (ITUT-X701, 1997)

Management systems exchange information modelled in terms of Managed Objects (MOs). Similar to the OSI definition, MOs are conceptual views of actual resources (both physical and logical) that are being managed or support certain management functions. Object-oriented principles apply to the information modelling of MOs, but should not have any impact on the internal implementation of the telecommunications management system.

3.1.4 CIM

The Common Information Model (CIM) applies basic structuring and conceptualisation techniques from the object-oriented paradigm to describe the management of systems and networks. A uniform modelling approach and the inherent properties of object-oriented descriptions support the co-operative development of management schema.

CIM provides a schema with respect to classification and association. This allows the managed environment to be described in a common framework. This framework is comprised of several layers:

- The **Core Model** represents information that is applicable to all areas of management.
- The **Common Model** represents information that is common to particular areas of management.
- The **Extension Schema** represents information extensions that are unique to specific technologies or environments.

In a similar fashion to SNMP, OSI and TMN, the Manager-Agent dynamic exists, but the main focus of the architecture is built around the Core Model, the Common Model and the Extension Schema. (DMTFa, 1999)

3.2 Communication Services, Protocols and Formats

3.2.1 SNMP

The Simple Network Management Protocol (SNMP) was (originally) designed for the management of networks based on Internet Protocols (IP). In a similar fashion to Internet communications, it operates on a connectionless basis. Management operations are performed through a series of retrieve ("get") and alter ("set") functions. The number of these commands continues to grow, however the semantics of the syntax is quite complex and does not interoperate well with non-SNMP systems.

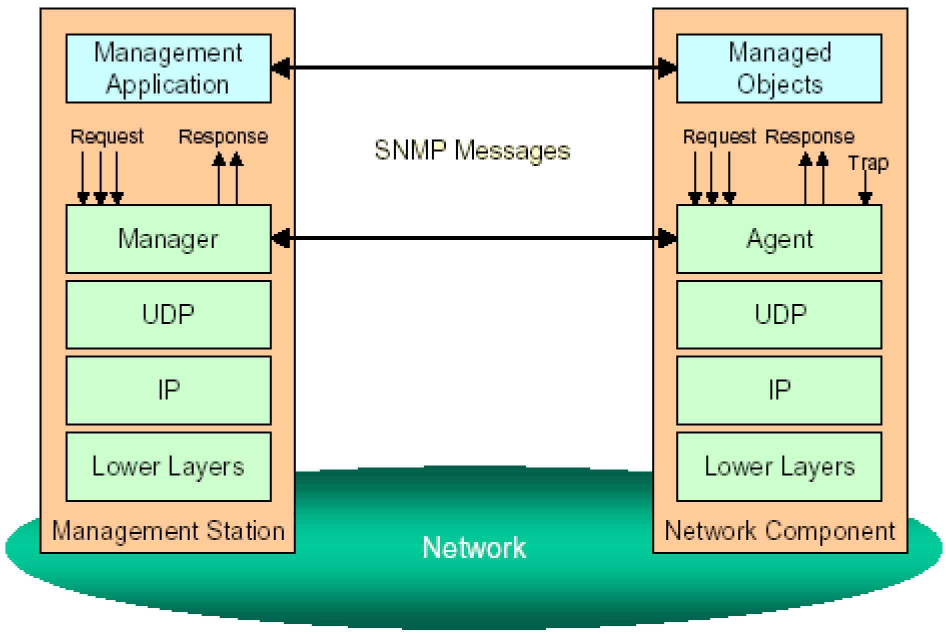

Figure 3.2.1.1 SNMP Communications Architecture

3.2.2 OSI

Since X.700 is an abstract notation, it is not bound to any particular technology when dealing with communications. However, there are strict guidelines in the specification as to how communication is to take place. Both connection and connectionless oriented transmissions can take place between MOs, provided both MOs support the protocols. The OSI Management Architecture also provides a management syntax that can be used describe the messages between MOs.

Communications in X.700 is provided by the Common Management Information Service (CMIS). CMIS provides the means for the exchange of information in management operations and notifications for management purposes in a common and standardised manner. CMIS uses the Common Management Information Protocol (CMIP) to transfer messages between MOs. Two types of information transfer can take place: Management Notification Service and Management Operation Service.

The behaviour of the communicating entities is dependent upon the specification of the MOs at which the notifications/operations are directed and is outside the descriptive scope of the CMIS. However, certain standard operations (such as GET and SET operations) that are used frequently within the scope of systems management are defined by CMIS.
(ITUT-X710, 1997)

3.2.3 TMN

TMN systems support the concept of interworking. That is to say that Management System A can communicate with Management System B. In order to interwork, communicating management systems must share a common view or understanding of certain management information, known as Shared Management Knowledge (SMK). This SMK provides the means by which disparate management systems can interface with one another. The logical concept of SMK can exist independently of the actual physical implementation. This is particularly the case for hierarchical management where a logical layered approach is taken.

It is necessary for a TMN system to support a wide variety of management areas, which cover the planning, installation, operations, administration, maintenance and provisioning of telecommunications networks and services. A TMN system should have the following functional abilities:

- to exchange management information between the telecommunications environment and the TMN environment
- to exchange management information between TMN environments
- to convert management information from one format to another so that information within the TMN has a consistent nature
- to transfer management information between locations within the TMN environment
- to analyse and react appropriately to management information
- to manipulate management information into a form which is useful and/or meaningful to the management information user
- to ensure secure access to management information by authorised management information users

(ITUT-M3010, 2000)

3.2.4 CIM

CIM provides a set of legal statement types that can be used to describe management operations in the information model or management schema. CIM is structured in a way such that the managed environment can be viewed as a collection of interrelated systems. Each of these systems is comprised of a number of elements, which can be described using the CIM syntax.

Management data is collected, stored and analysed using a common XML format. By using this common standard, 3rd parties can develop value-added functions that may be easily integrated into the managed system.
(DMTFa, 1999) (DMTFb, 1999)

3.3 Core Services and Application Services

3.3.1 SNMP

An SNMP entity (Manager, Agent) is comprised of an Engine and one or more Applications. The SNMP Engine is made up of the following subsystems:

1. The **Dispatcher** is a key component in the SNMP engine. Its dispatches tasks to the multiple version-specific Message Processing Models and sends PDUs (Protocol Data Units) to various applications. There is only one Dispatcher in an SNMP engine.
2. The **Message Processing Subsystem** is responsible for preparing messages to send and extracting data from received messages. An Engine can contain multiple Message Processing Models.
3. The **Security Subsystem** provides security services such as authentication and messages privacy. An Engine can contain multiple Security Subsystems.
4. The **Access Control Subsystem** provides authorisation services by means of one or more Access Control Models

(Harrington, Presuhn & Wijnen, 1999)

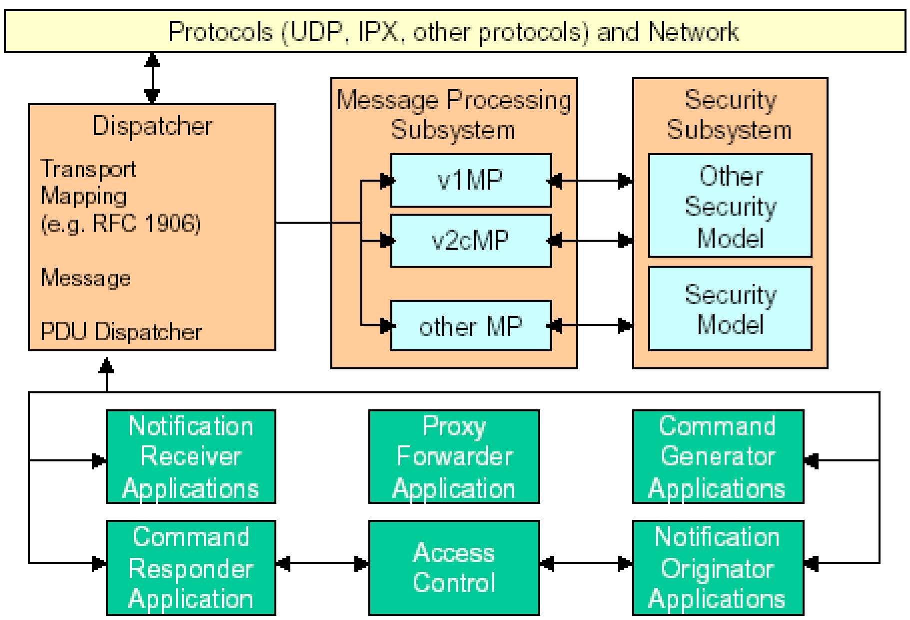

Figure 3.3.1.1 SNMP Engine

In an SNMP deployment, Managers and Agents comprised of the identified subsystems and applications communicate and collaborate with one another to manage network traffic, resources, etc.

3.3.2 OSI

The role of OSI management is categorised into a number of functional areas: Fault Managements; Configuration Management, Accounting Management; Performance Management and Security Management. These are often collectively referred to as FCAPS functionality.

Fault Management is concerned with fault detection, isolation and the correction of abnormal operations in the managed network environment. Faults can cause systems to fail to meet their operational objectives and usually manifest themselves as errors. Fault management includes functions that maintain and monitor error logs, accept and respond to error notifications, identify faults, carry out diagnostic tests and correct faults (where possible).

Configuration Management identifies, exercises control over and exchanges data with systems for initialising, providing and terminating interconnecting services. It includes functions to control normal operations, associate names with MOs and sets of MOs, start and stop MOs, collect information on demand about current conditions and to change configurations of services.

Accounting Management enables charges to be incurred for the use of resources with the managed network environment and for resource costs to be identified. Accounting Management includes functions to inform users of costs incurred, resources consumed, enable accounting limits to be set and tariff schedules to be associated with the use of resources and enable costs to be combined where multiple resources are utilised to achieve a given communication objective.

Performance Management enables the behaviour of resources in the managed network environment and the effectiveness of communication activities to be evaluated. It includes functions to gather statistical information, maintain and examine logs of system histories, determine system performance and alter system operation modes to conduct performance management activities.

Security Management supports the application of security policies by means of functions which include the creation, deletion and control of security services and mechanisms, the distribution of security information and the reporting of security events.
(ITUT-X701, 1992)

3.3.3 TMN

A TMN system is comprised of a set of functional building blocks; Operations Systems Function (OSF), WorkStation Function (WSF), Mediation Function (MF), Network Element Function (NEF) and Q Adaptor Function (QAF). Operations take place between these blocks to achieve the functional goals of a TMN system. A Management Application Function (MAF) represents part of the functionality of one or more TMN management services. Each functional block has a set of MAFs associated with it:

1. **Mediation Function**. The MF-MAF is used in the support of Manager and Agent roles. MF-MAFs are optional and are used to provide supportive functionality in OSF. Examples of such functions are temporary storage, filtering, thresholding, etc.
2. **Operations Systems Function**. These management applications functions are the essential and underlying aspects of management functionality blocks. The range from simple to complex functions, such as:

- Support of Manager and Agent roles in access to managed object information
- Adding value to raw information (e.g. data concentration, statistics, performance analysis, etc)
- Reaction to incoming information (e.g. automatic reconfiguration, fault tracking, etc)

3. **Network Element Function**. These management application functions are present in the NEF primarily to support the Agent role.
4. **Q Adaptor Function**. These management application functions are present in the QAF primarily to support the Manager and Agent roles.

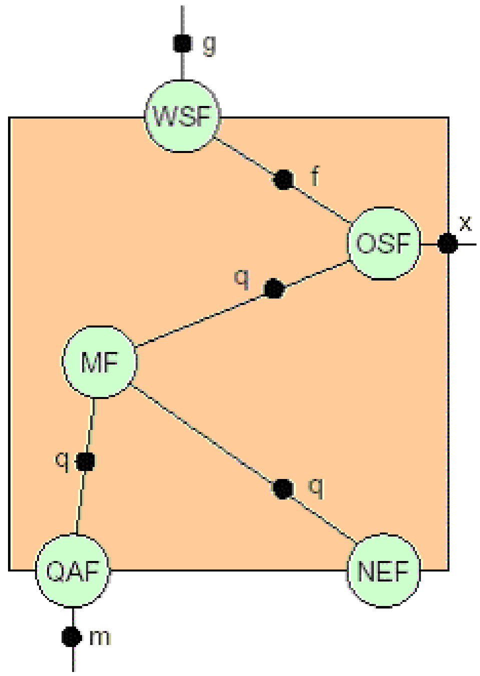

Fig 3.3.2.1 Reference Points (ITUT-M3010, 2000)

In order to illustrate connections between function blocks, the concept of **Reference Points** is introduced. Reference points define the interface characteristics for information exchange between function blocks. Each of these is a high level abstraction of communication and they do not dictate implementation protocols.

- The **q reference point** illustrates the logical part of the information exchange between function blocks, as defined by the information model mutually supported by the functions.
- The **f reference point** is used to denote information exchange between WSF and OSF blocks and/or WSF and MF blocks.
- The **x reference point** is used to illustrate communication between the OSF function blocks in different TMNs.
- The **g reference point** is used to denote communicate between human users and the WSF. It is not considered to be part of the TMN, even though it conveys TMN information.
- The **m reference point** is located between the QAF and other non-TMN managed entities or managed entities that do not conform to TMN standards.

To decrease complexity when defining a logical telecommunications management architecture, TMN is considered to be separated into logical layers. This **Logical Layered Architecture** (LLA) is a concept for the structuring of management functionality into four layers, where each layer restricts management activities within its boundaries in accordance with clear definitions, based on business, service, network and element management. The **Business Management Layer** (BML) has responsibility for the proprietary functionality of enterprise. The BML is included in the TMN architecture to facilitate the specification of capability that it requires of the other logically lower layers. The **Service Management Layer** (SML) is concerned with the services that are provided to customers. Some of the main functions of this layer are service order handling, complaint handling and invoicing. The **Network Management Layer** (NML) has the responsibility for the management of a network as supported by the Element Management Layer. Functions addressing the management of a wide geographical area are

said to be contained in this layer. It has complete visibility of the whole network and a technology independent view is provided for the SML. The **Element Management Layer** (EML) manages the Network Elements (NE) encompassed by the TMN system. It provides an abstract representation of NEs for the NML. Below the EML, the Network Elements are said to exist, but they are not considered a separate layer themselves.
(ITUT-M3010, 2000)

3.3.4 CIM

Since CIM is an abstract notation, there are no directly implemented services available. However by following the notation guidelines, some useful structures can emerge.

A Directory Enabled Network (DEN) provides the building blocks for mapping users to network services, and business criteria to network services. Applications and services are able to leverage network infrastructure on the user's behalf to assist with service creation, maintenance and management. The central information repository of a DEN is directory where the intersecting relationships of users, applications and network services are defined. Networked applications are managed by associating users and applications with a set of resource policies. The DEN is used by the DTMF to describe cross-domain solutions.

The Web-Based Enterprise Management (WBEM) is an initiative to provide web access to enterprise management information and systems. Since the goal of the DTMF is to tie industry organisations and standards together, the WBEM is now part of the overall DTMF strategy. The DMTF have defined a mapping of CIM operations onto Hyper Text Transfer Protocol (HTTP) to allow WBEM operations to be performed in an open and standardised manner.
(DMTFa, 1999) (Carey & O'Reilly, 2002)

3.4 Relevance to M-Zones

A good analogy of Smart Spaces is the idea of a series of unconnected islands. Each of these islands represents a smart space, operating independently of one another. An architecture is required to allow these unconnected islands to interoperate in a cohesive and useful fashion. Smart Spaces using well-designed management architecture(s) would allow domains to exchange information, perform remote tasks and provide a greater level of functionality than Smart Spaces operating with no overall functional structure. Each smart space is based primarily upon its own network, which will most likely be IP based. Networks based on IP principals are the industry standard when referring to computer networks. Telecommunications networks are also moving in this direction, with both GPRS and UMTS being IP based. Smart Spaces are building upon computer and telecommunications technologies, so it would be logical to assume that they will also be IP based. It is important to study existing IP network management techniques and identify the aspects of them that may be applied when defining this architecture for interconnecting disparate zones.

From SNMP the most important lesson is simplicity. It is relatively easy to implement an SNMP compliant network and very few modifications need to be made to resources to become part of the managed network. However, SNMP places most of the burden on the Manager component and keeps the Agent relatively "light". In a multi-zone scenario, this may not be a scaleable solution, since a management component may serve many agents over a large area. In the event of a fault and the manager were unable to communicate with the agent, the local managed zone may cease to function. If the agent were sufficiently autonomous, it would be able to continue most of its activities while the manager was offline. Any messages for the manager could be stored in a buffer and sent at a later time.

The connection-less aspects of SNMP are also quite interesting. Current Smart Spaces technologies are based mostly around wireless networking technologies, such as 802.11, Bluetooth and Infrared. Due to the large number of devices potentially present in a Smart Space and the transient nature of many of these elements, it is logical to assume that Smart Spaces will continue to predominantly use wireless communications methods. In a busy Smart Space with devices frequently entering and leaving, network connections will be established and broken at a much higher rate than traditional wired networks. In this way, it will be difficult to maintain connection-oriented communication protocols.

An M-Zones architecture will certainly be a more complex network management definition than SNMP, due to the increased physical network complexity, greater management functional scope and broader service definitions. However the underlying ideas of robustness and network element autonomy are important issues to consider when defining this network management system.

The OSI X.700 network management architecture presents some characteristics that may be useful when describing an ubiquitous networking architecture. The most notable are FCAPS functionality and the object-oriented hierarchical structures. The FCAPS model provides a clear set of functional objectives that must be achieved. Although FCAPS functionality may not map directly to pervasive environments, the principals of fault, configuration, accounting, performance and security management would be useful guidelines when outlining pervasive architecture(s).

X.700 presents two hierarchical structures for consideration. The object model class structure offers an abstract view of the network in an uninstantiated or ideal form. This is useful when describing a defined architecture as a separate entity to the actual physical network and network elements. The object model name-binding scheme presents a model of the actual instantiated objects and offers a representation of an actual working system. These two models will differ in appearance, but certain hierarchical similarities will exist. It is useful to compare the abstract ideal system with an actual working system. A similar approach would be useful when describing a Smart Space network management architecture, to highlight areas in which the abstract model differs from the implemented system.

The inheritance concept could also be useful when addressing the idea of an evolving network. As technologies advance, management architectures must adapt to suit more radical changes. A modular, object-oriented approach would allow certain components to be "upgraded" without requiring any great change to the overall architecture. One drawback of the OSI network management architecture is the lack of real world implementations. This would indicate that OSI is perhaps too complicated or flawed to exist in the real world? Or perhaps IP networks have thus far not required an architecture that offers as much functionality? Whatever the case, X.700 appears to offer some useful guidelines and raise important issues which will need to be addressed when developing a multi-domain management architecture.

The most striking aspect of TMN is the huge complexity of the architecture, as shown in Sections 3.1.3, 3.2.3 and 3.3.3. A trend of increasing complexity can be clearly seen when comparing and contrasting SNMP, OSI X.700 and TMN with one another. However, TMN also brings with it a very well defined and tested architecture, which can be somewhat lacking when discussing computer network management architectures. TMN is based upon the X.700 model as described earlier, hence many of the characteristics highlighted as being of importance to the M-Zones project are also applicable here. The Manager, Agent and Managed Object dynamic can be clearly seen again, cementing the view that this model is of particular importance. Considering Managers, Agents and Managed Objects, there is an immediate network management abstraction with respect to ubiquitous devices.

One of the most important aspects of TMN that has direct relevance to M-Zones is the way in which it deals with the concept of interworking and inter-domain communication. The SMK (Shared Management Knowledge) concept described in Section 3.2.3 is certainly worth investigating. Defining communication interfaces for every possible inter-zone communication scenario may be an impractical solution when dealing with Smart Space systems, however this model warrants further study. Of equal importance is the Reference Point concept, specifically the x and m points which deal with information exchanges outside of the TMN environment. When dealing with Smart Spaces, a set of interfaces to networks that are not necessarily Smart Spaces themselves will be required and lessons can be learned from TMN approach to communication with other TMN and non-TMN environments.

The layering model as outlined by the LLM is an abstraction that may prove useful when attempting to define logical pervasive management applications. If applications can be defined with an abstract vision, management issues may be highlighted, than by merely defining applications in terms of network elements, mangers, agents etc. Also the concept that the layer definitions may or may not dictate physical implementation strategies is worth noting. Physical implementation techniques are often incompatible with logical modelling and a separation of the two could be quite useful, especially with respect to emerging and untested ubiquitous devices and standards. Many other aspects of TMN do not concern themselves with implementation issues, which reinforces this view. When defining a multi-domain management architecture for Smart Spaces, it will be important to assume an abstract position. Focussing on implementation-specific issues may cause more general management issues to remain unstudied. Also adopting this broader view may allow for many abstract architectures to be considered, as opposed to one all-encompassing network management system. It may be the case that different Smart Spaces will require different degrees of management architecture, based on requirements. E.g. A Smart Space in a café that offers wireless Internet access to its customers will not require as much management as a Smart Space in a shop that allows customers to pay for goods directly from their bank account (e.g. Smart Space debit ‘card’). Logically, the shop would require greater levels of authentication and security in its Smart Space management system than the café. Will they both use one system; different versions of one system; or totally different systems? This is an important question to ask when beginning to develop management architecture(s) for Smart Spaces.

TMN highlights many issues that need to be considered when describing Smart Space network management architecture. Any architecture(s) produced by M-Zones will not be as rigid as TMN, because they will need to be suitably flexible to adapt to different Smart Spaces. Again, this raises the issue as to whether there will be many architectures or one all-encompassing system. Further research is required in this area. Another important issue to highlight, is that it is any architecture(s) developed by the M-Zones projects must be able to interface and communicate with other managed networks (e.g. TMN, SNMP) to provide a genuinely ubiquitous service. Knowledge of these systems will be required when detailing these interfacing components.

The CIM as proposed by the DMTF highlights some issues that deserve consideration. The fact that CIM is an abstract notation reduces the real-life implementation lessons that can be learned. However, due to the constantly evolving industry environment, basing an architecture on any one technology would not be prudent. An architecture specifically designed for a single technology needs to evolve with this very technology or it will become obsolete when the technology becomes obsolete. This approach is not desirable for Smart Spaces management architecture(s) as they must operate in a heterogeneous and dynamic technical environment. However, as mentioned with respect to both X.700 and TMN, creating an architecture model that is not implementation specific (but has implementation guidelines) may prove to be effective.

CIM can be used a mediation technology between multiple networks. The WBEM initiative bears a lot of relevance to the practical stages of the M-Zones project. WBEM applications use standard Internet technologies and protocols to provide implementations of management systems. The fact that these technologies are well defined and tested could be useful when implementing an M-Zones architecture. Web-based applications would be ideal during the implementation stages of the project due to the fact that many are freely available and well supported.
The Extension Schema also provides an interesting aspect. This allows 3rd party organisations to add components as they see fit. Allowing a Smart Space architecture to be extensible might assist in industry adoption and encourage other developers to create services that interact with it. The use of XML as a communications standard within the CIM is also worth noting. XML is a standard mark-up language that has gained a lot of popularity and is widely used in many systems. This highlights XML as a possible candidate for a messaging standard within any Smart Space architectures that the M-Zones project may produce.

3.5 Similar Work

The eBiquity research group from the University of Maryland Baltimore County undertook the task of providing an infrastructure and communication protocol for wireless services. The architecture developed by the **Centaurus** project consists of a number of components that facilitate communication between portable devices and the Centaurus System (CS) within a confined space. The Communications Manager (CM) handles all communications between the client and the rest of the Centaurus system. The Service Manager (SM) acts as a mediator between clients and services and is responsible for client and server registration, service leasing and service discovery. The communication medium used by the Centaurus project is a derivative of XML, which they named Centaurus Communication Markup Language (CCML). They also developed Centaurus Communication Protocol (CComm), which was used to communicate with mobile clients and services. The Centaurus project ended in 2001 and was superceded by Centaurus 2 (Undercoffer, Cedilinik, Perich & Joshi, 2001) and Vigil (Kagal, Undercoffer, Perich, Finin & Yesha, 2001). However, both of these projects have concentrated on security aspects of pervasive computing.
(Kagal, Korolev, Chen, Joshi & Finin, 2001)

The most interesting aspect of Centaurus from an M-Zones point of view, is their use of XML when developing a their communication language. XML is a very simple text-based standard that most platforms can understand. It is lightweight and few resources are required to read/write XML documents. When dealing with many ubiquitous entities of differing computational ability, it is important to ensure that entities of similar complexity can communicate as easily with each other as entities with a simpler design and vice versa. XML presents a strong argument for itself when deciding on standards for communication. It is very well defined and tested and there is a lot of software freely available that supports it. The Centaurus project is limited in its relevance to M-Zones since it only concerned itself with managing services in a single smart space. However, it highlights the need for management at the local level. Inter-domain management is just a step above managing a single domain and any M-Zones multi-domain architecture will have to interoperate with local Smart Space management systems. This reinforces the idea that M-Zones should concern itself with both intra and inter zone management.

4. Future Directions

There are many potential rewards as a result of developing management structures that successfully allow components to inter-operate with each other across multiple domains. The explosive growth of the World Wide Web and its corresponding increase in popularity and subsequent development of Internet technologies illustrates just how powerful large scale networks can be. Smart Spaces present an opportunity to expand the reach of computer networks into areas previously thought to be inaccessible. New services, models and usage practices may develop as a result of this, furthering the impact of Information Technology in people's lives.

The ultimate goal of this research topic is to produce a new type of management architecture. It is difficult to imagine that Smart Spaces could be adequately managed by any of the management technologies described. However, the initial step to be taken when attempting to create a new management structure is to study existing architectures. The most immediate problem when surveying these management architectures is identifying areas that bear relevance to the field in question and isolating the subsections that are of particular interest. Lessons learned from studying SNMP, X.700, TMN and CIM (and to a lesser extent the Centaurus project) will prove invaluable to the M-Zones project when attempting to develop its own Smart Space network architecture(s). From SNMP, simplicity is the key recognisable factor. An architecture that becomes bloated will most likely become too complicated to be useful. The connectionless communication methods used by SNMP are also worth noting because of the higher frequency of broken connections in wireless networks. The OSI X.700 management architecture presents a level of abstraction not seen in SNMP. A management notation method that is separate from implementation may prove effective when dealing with pervasive environments. Unlike traditional computing networks, which remain relatively stable in terms of connected devices, Smart Spaces will be ever-changing with devices constantly entering and leaving the environment. This would be very difficult to model without a certain degree of abstraction. The FCAPS functionality described by X.700 is also a good guideline that may be used when attempting to develop functional aspects of Smart Space architecture(s). From TMN, there are lessons to be learned regarding inter-working and inter-domain communications. Smart Space management architecture(s) may not be quite as rigid as TMN, but they will certainly share characteristics, especially in this respect. The most important aspect of note from the DMTF's CIM is the use of a common messaging standard. This highlights the issue of the need for a standard messaging protocol in Smart Space environments. Since devices will have varying degrees of complexity and processing abilities, simplicity will again be a key issue. The WBEM initiative illustrates some initial steps that may be taken when the M-Zones project moves into the practical experimentation phase.

The next step in this field of research is to study some ubiquitous technologies and catalogue areas that are of particular importance to management. As a result of this, some experiments will be conducted with Smart Spaces with a vision to producing some preliminary management architectures. Over the lifecycle of the project, various views, iterations and versions of architectures will be presented. It is the goal of the project to provide multi-domain network management systems that can assist in the delivery of ubiquitous services and provide the user with a seamless Smart Space experience.

5. References

Carey K., O'Reilly F., 2002, "Heterogeneous Tools for Heterogeneous Network Management with WBEM", DMTF Developers Conference 2002, San Jose. Adaptive Wireless Systems Group, Department of Electronic Engineering, Cork Institute of Technology, Cork, Ireland.

Case J., Fedor M., Schoffstall M. and Davin J., May 1990, "A Simple Network Management Protocol", RFC 1157.

Case J., Mundy R., Partain D. and Stewart B., April 1999, "Introduction to Version 3 of the Internet-standard Network Management Framework", RFC 2570.

Case J., Harrington D., Presuhn R. and Wijnen B., April 1999, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2572.

DMTF, Distributed Management Task Force, http://www.dmtf.org

DMTF, June 14, 1999: Common Information Model (CIM) Specification. DMTF, Version 2.2.

DMTF, July 20, 1999: Specification for the Representation of CIM in XML. DMTF Version 2.0

Harrington D., Presuhn R., and Wijnen B., April 1999, "An Architecture for Describing SNMP Management Frameworks", RFC 2571.

ITU-T Recommendation M.3000, February 2000: Telecommunications management network Overview of TMN Recommendations.

ITU-T Recommendation M.301, February 2000: Telecommunications management network – Principles for a telecommunications management network.

ITU-T Recommendation X.200, July 1994: Information Technology – Open Systems Interconnection Basic Reference Model: The Basic Model. International Telecommunication Unit, Geneva, Switzerland.

ITU-T Recommendation X.200, 1993: Open Systems Interconnection – Model and Notation – Specification of Abstract Syntax Notation One (ASN.1). International Telecommunication Unit, Geneva.

ITU-T Recommendation X.210, November 1993: Information Technology – Open Systems Interconnection – Basic Reference Model: Conventions for the Definition of OSI Services. International Telecommunication Unit, Geneva.

ITU-T Recommendation X.500, 1993: Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. International Telecommunication Unit, Geneva.

ITU-T Recommendation X.501, August, 1997: Information Technology – Open Systems Interconnection – The Directory: Models. International Telecommunication Unit, Geneva.

ITU-T Recommendation X.700, September 1992: Management Framework for Open Systems Interconnection (OSI) for CCITT Applications. International Telecommunication Unit, Geneva.

ITU-T Recommendation X.701, 1997: Information technology – Open Systems Interconnection – Systems management overview.

ITU-T Recommendation X.710, 1997: Information technology – Open Systems Interconnection – Common management information service.

ITU-T (CCITT) Recommendation X.720, 1992: Information technology – Open Systems Interconnection – Structure of management information: Management information model.

ITU-T (CCITT) Recommendation X.721, 1992: Information technology – Open Systems Interconnection – Structure of management information: Definition of management information.

ITU-T (CCITT) Recommendation X.722, 1992: Information technology – Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects.

Kagal L., Korolev V., Chen H., Joshi A., Finin T., April 2001. "Project Centaurus: A Framework for Indoor Services Mobile Services." In Proceedings of International Workshop on Smart Appliances and Wearable Computing (IWSAWC) at The 21st International Conference on Distributed Computing Systems 2001. Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore MD, USA.

Kagal L., Undercoffer J., Perich F., Finin T., Yesha Y., October 2001. "Vigil: Providing Trust for Enhanced Security in Pervasive Systems." Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore MD, USA.

Undercoffer J., Cedilinik A., Perich F., Joshi A., June 2001 "Centaurus 2: A secure infrastructure for multi domain service discovery and utilization." Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore MD, USA.

Zimmermann, H, 1980. OSI Reference Model -- The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications.