TMN and Telecommunication Networks Testing

Mahamat Guiagoussou[1], Michel Kadoch[2]

1. Centre de Recherche Informatique de Montréal
1801, avenue Mcgill College, Montréal, Québec, H3A 2N4
Canada
mguiagou@crim.ca

2. École de Technologie Supérieure
1100, rue Notre-Dame Ouest, Montréal, Québec H3C 1K3
Canada
kadoch@ele.etsmtl.ca

Abstract

The objectives of the paper is to review the conflicting requirements and needs of existing telecommunication network testing approaches, services and equipment, in order to provide a simple but powerful solution that allows automated and standardized testing activities. We present in the paper a progressive transition from the current proprietary practices, to a distributed and fully TMN compliant management of telecommunication networks testing.

Keywords

TMN, OSI, Network testing, CMIS/CMIP, Network Performance, RTU

1. INTRODUCTION

Before the deregulation and the privatization of telecommunication industries, telecommunication network management was simpler. With the telecommunication areas rapid changes, multiple vendors and technologies interoperability, new services

A. Petrenko et al. (eds.), *Testing of Communicating Systems*

and technologies integration became the biggest challenge of telecommunication networks and services management [11]. A completely automated management is almost impossible and unrealistic. The provisioning of an automated system removes the crucial need for human operator intervention.
Telecommunication Network Management (TMN) addresses the need for automation by providing standardized machine-to-machine interfaces that replace current manual functions and allows a management of heterogeneous equipment [1, 2]. By providing general and flexible interfaces, it also addresses the need to support rapid evolution of technology and integration of new services [3, 6]. For the interest of testing, two recommendations have been proposed by OSI/TMN standards : the *X.745* (Test Management Function) [7] and the *X.737* (Categories of Diagnostic and Confidence Tests) [8].
The automation of management aspects such as testing and faults diagnosis is a key issue in Telecommunication Network and Service Maintenance. Current telecommunication maintenance and fault management activities consist in continually monitoring the network elements and services. When troubles are experienced by users, they are notified to the network operation centers or to a help desk. Field personnel are sent to make manual measurements and tests in order to troubleshoot the problems and restore the affected services.
The objectives of the paper is to review the conflicting requirements and needs of existing telecommunication network testing approaches, services and equipment, in order to provide a simple but powerful solution that allows automated and standardized testing activities. We present in the paper a progressive transition from the current proprietary practices to a distributed and fully TMN compliant management of telecommunication networks testing.

2. REVIEW OF TMN FROM TESTING PERSPECTIVES

This section presents an overview of TMN principles, standards, and architectures. It also presents standards recommendations defined for testing management. Then driven forces for TMN deployment are discussed.

2.1 Overview of TMN

2.1.1 Evolution and Objectives

TMN have been introduced by ITU-T, and defined in recommendations M.3000 [1], and M.3010 [2]. Standardization studies started in 1985 with the definition of interfaces and the specification of interface protocols between Operation Systems (OSs) and transmission terminals. In 1988 the first recommendation M.30 was included as part of the blue book. Extension was then provided to include the management of all telecommunication networks and services. In 1992 M.3010 [2], the revised version was published. TMN also provides a structured architecture for the interconnection of OS (Operation system) and/or telecommunication equipment in order to allow management information exchanges. These interconnections use standardized interfaces including protocols and messages. The basic objectives of TMN focus on: the use of generic telecommunication network models for the management of heterogeneous network

services and equipment; the operation across multiple vendors and different technologies; the inter-working among the multiple management and operation systems; and the management of inter-working among separately managed networks or domains.

2.1.2 Functional Architecture

Functional architecture describes the appropriate distribution of functionality within TMN [2, 4]. These functionality were defined as functional blocks, namely : Operation System Function (OSF) processes information related to the telecommunications management; Network Element Function (NEF) which communicates with the TMN for the purpose of being monitored and/or controlled; Q-Adapter Function (QAF) is used to connect as part of the TMN those non-TMN entities which are NEF-like and OSF-like; Mediation Function (MF) acts on information passing between an OSF and NEF (or QAF) to ensure that the information conforms to the expectations of the function blocks attached to the MF; Work Station Function (WSF) provides the means to interpret TMN information for the management information user; and Data Communication Function (DCF) for the transfer of Telecommunication Network Management Information.

At the service boundaries of TMN function blocks, reference points are defined as access to services. They represent conceptual points of information exchanges between non overlapping functional blocks. Three main interfaces are defined within TMN : the q-class reference points (between functional blocks within TMN that can contain a management application) ; the f-class reference points (between a Work Station and TMN); and the x-class reference points (between OSF blocks of two TMNs or OSF block of a TMN and the equivalent function of another network). Figure 1 presents examples of reference points between functional blocks. The upper part illustrates reference points between a TMN block and a non TMN OSF (i.e., reference point m). The lower part gives more specific cases of reference points : the left one between users, a WSF, an OSF and a NEF, and the right one between an OSF and a QAF. In each case, the OSF use a q3 reference point to communicate via a MF which communicates in turn with the final blocks (NEF or QAF) using a qx reference point (a q interface with reduced functionality).

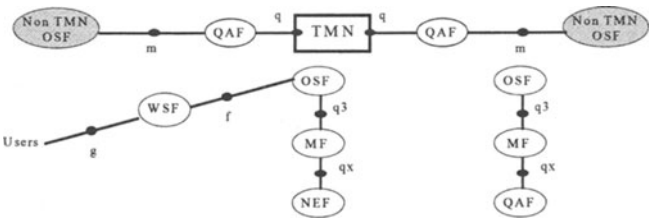

Figure 1 - Example of function blocks and reference Points

TMN identified a need for a hierarchy of management responsibilities. Such hierarchy can be described in terms of management layers. The scope of each layer is wider than the layer below it. In general, it is expected that upper layers will be more generic in functionality while lower layers are more specific. The Logical Layer Architecture

(LLA) [2] implies the clustering of management functionality into layers. It uses a recursive approach to decompose a particular management activity into a series of nested functional domains. Each functional domain forms a management domain under the control of an operation system function (OSF) and thus each domain is called an OSF domain. A domain may contain other OSF domains to allow further layering and/or it may represent resources (logical or physical) as managed objects (MOs) within that domain. All interactions within a domain take place at generic q reference points. However, interactions between peer domains, i.e. crossing an OSF domain boundary, can take place at a q or x reference points depending upon the business strategy applicable for that interaction. When providing network services it is common for management to cross the boundaries of an Administration, hence arrangements are made for inter-TMN interactions.

2.1.3 Information architecture

In order to allow effective definition of managed resources, the TMN methodology makes use of the OSI system management principles and is based on an object-oriented paradigm. Management systems exchange information modeled in terms of managed objects [9]. As illustrated in Figure 2, managed objects collected within a Management Information Base (MIB) are conceptual views of the resources that are being managed or may exist to support certain management functions (e.g. event forwarding or event logging). Thus, a managed object is the abstraction of such a resource that represents its properties as seen by (and for the purposes of) management processes. A managed object may also represent a relationship between resources or a combination of resources (e.g. a Network). It must be noted that object oriented principles apply to the information modeling, i.e. to the interfaces over which communicating management systems interact and should not constrain the internal implementation of the telecommunications management system.

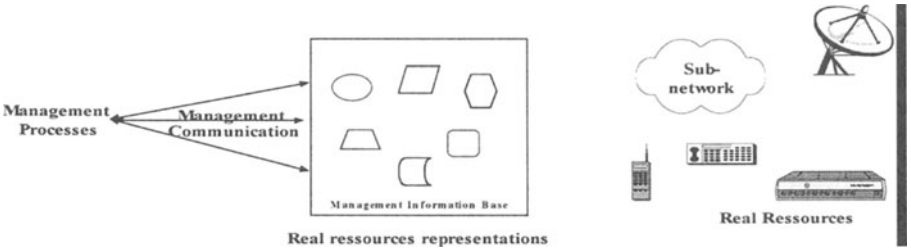

Figure 2 : Real resources modeling and management information base

An object in the perspective of TMN/OSI management is defined by: the attributes visible at its boundary; the management operations which may be applied to it; the behavior exhibited by it in response to management operations or in reaction to other types of stimuli and notifications that are emitted when some internal (e.g. threshold crossing) or external (e.g. interaction with other objects) occurrence affecting the object is detected. The value of these attributes and the interactions the object can have with its management environment define its behavior. For example, such interaction could occur when an operation requests is received from a manager via an agent or when

results are sent back in response to a given request after an action have been performed. The GNIM (Generic Network Information Model) [6] provides management of the inter-operability of services, networks, NE, OS, etc. It also provides a uniform management information model. It is a technology independent model that can be applied to different types of equipment that use common and standardized interfaces. Management of a telecommunications environment is an information processing application. Because the environment being managed is distributed, network management is also a distributed application. This involves the exchange of management information between management processes for the purpose of monitoring and controlling the various physical and logical networking resources. The Manager/Agent concepts, developed for OSI systems management, are introduced in TMN framework. The concepts necessary for the organization and interworking of complex managed systems (e.g. networks) are also introduced under the headings of management domains and shared management knowledge. For a specific management association, the management processes will take on one of two possible roles defined in X.701 [4]. The Manager role describes the part of the distributed application that issues management operation directives and receives notifications, while the agent role describes the part of the application process that manages the associated managed objects. The role of the Agent will be to respond to directives and requests issued by a Manager. It will also reflect to the Manager a view of these objects and emit notifications reflecting the behavior of these objects. A Manager is the part of the distributed application for which a particular exchange of information has taken the manager role. Similarly, an Agent is the part that has taken the agent role. The managing entity uses the Common Management Information Protocol (CMIP) to access managed information provided by an agent residing either in a stand alone open system or in the managed resource.

2.1.4 Physical Architecture

Physical architecture describes implementation of reference points (i.e., interfaces) and examples of physical components within TMN. For each functional block a physical blocks can be implemented thus leading to a physical architecture. These physical blocks are: Operation System (OS); Network Element (NE); Q-Adapter (QA); Mediation Device (MD); Work Station (WS); and the Data Communication Network (DCN). Reference points are realized within the physical architecture by physical interfaces within system or equipment. They are represented by capital letters (Q, F, X) and form the common boundary between associated building TMN blocks. The F interfaces can be found between WS and the TMN, the Q (Q3) interface between TMN devices and the X interface between TMN devices of one TMN with devices of another TMN via DCN.

2.2 Standards for Telecommunication Networks Testing

Two standards for the purpose of telecommunication networks tests are presented: X.745 (Test management function) and X.737 (Categories of Diagnostic and Confidence Tests).

The X.745 [8] specification describes the needs for the remote control of testing activities and defines a framework for the specification of tests to be applied to resources including open systems. A test is considered as the operation and monitoring of open systems or their parts, in a specified environment in order to collect information on the functionality and/or the performance of the considered system(s). A test is defined with the creation of the environment for the test to be performed, the control and the monitoring of the considered systems (i.e. operations of the test), the modification of a normal operational environment. The test control includes for example the need to suspend, resume and terminates the test. Actually, tests equipment available in the market does not allow to automatically suspend, nor to resume the tests they perform.

Each test is defined with a unique identifier in such a way that data generated by the same test can be traced and correlated. Parts or aspects of the system environment that can require alteration for the purpose of the test are : the connections to other open systems; the configuration of the tested system; the traffic load required by the tested system; and the configuration of the testing systems and instruments. In some cases, test scheduling mechanisms are required. A test can also be specified in such a way that it is activated when some predefined conditions are satisfied (i.e. a threshold is reached) or when a specific event is detected (i.e., an Alarm Indication Signal).

Specification of a test includes the description of its *objectives*, its *environment*, its *controllability* (synchronous, asynchronous), and the *testing procedures* and *tests states*. The execution of a test involves two or several application processes. The manager-agent paradigm is used to define these processes: the managing process is concerned with the test initiation (it is called *test conductor*), and the agent process is allocated the task of executing the tests (it is called *test performer*). The test performer is requested by the test conductor to realize the test. A simplified architecture of the test management is depicted in Figure 3. A test request is sent to a managed object in the test performer. This later has the ability to receive and respond to the test request. Such a functionality is called TARR (Test Action Request Receiver). The managed objects that provide management view of the object under test (MOT) such as the telecommunication circuits to be tested, are identified within the test request. Each test must use one or several MOT(s). Additional information representing management or managed resources that are used for the need of testing (insertion and test signal reception points) such as Remote Testing Units (RTU) defined as AO (Associated Object). Information collected during the execution of the tests are specified and stored in support objects called TO (Test Object).

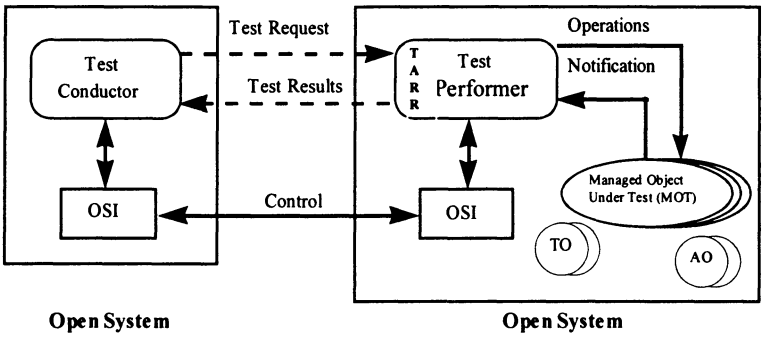

Figure 3 : Simplified Test Management Architecture

The X.737 specification [7] defines a set of basic tests for the categories of tests for the service introduction and faults diagnostic. These test are used to verify the ability of a specific equipment, a system or a network to realize correctly its allocated function (i.e., the tested entity continues to behave properly as defined in its specification). The specifications also define the way these tests are achieved and notifications are used to detect faults in order to isolate the cause of problems. These tests can be classified as follow: resources tests category (*resource boundary test, resource self test),* communication path tests category (*loop-back test, far-end connection test, connectivity test, connection test, delay, data integrity test)*; protocol integrity test; and test infrastructure test.

In order to use these generic tests in current telecommunication environment, additional specialization and refinement are required. Explicit tests selection must be specified. The advantage of an appropriate tests classification is that is ease the matching of test classes with well Known fault types, the reduction of faults diagnosis and troubleshooting complexity.

2.3 Motivations and driven forces for TMN deployment

2.3.1 General motivations

Several key drivers are forcing the deployment of TMN solutions in telecommunication networks management [10]. TMN standards and other related recommendations are becoming more and more stable. Telecommunication industries, R&D community, and software developer efforts reached so far an acceptable level of practical applicability. Distributed computing standards are now emerging. Computing technology such as CORBA have actually real time application oriented implementations (e.g., Orbix, Obeline, etc.) that are used in several domains. Software technologies and concepts such as: manager-agent mechanism, object oriented paradigm, intelligent multi-agent technologies, mobile agent theory, software reengineering and databases are widely used and deployed. Rapid prototyping, reduced development cost, and ease of use are some of the attracting opportunities provided by Web-Based Management for TMN. Intranet and Internet remote access facility are becoming the a promising tool for

remote and standardized management activities. Even if SNMP based management are more popular than CMIP, proxy products are available to allow the usability of TMN based protocols. Actually, number of TMN compliant OSs and NEs are made available by vendors, service provider, and equipment manufacturers. Artificial Intelligence and Expert System theory are now being actively used to help implementing human knowledge and expertise, and automate routine tasks.

2.3.2 Specific testing motivations

As telecommunication networks are growing in complexity, types, and dimension, their maintenance and specifically their testing poses a big challenge. From the later perspectives, several issues drive the advance of distributed and opened maintenance in telecommunication networks [14]. Wide area digital transmission facilities are used in corporate networks. Thus the requirements for appropriate network testing, drive the way these facilities are managed. Network quality is one of the national and international success and market competitiveness criteria for enterprises and organization. Network missions are critical; any trouble that disrupts a service can seriously affect productivity. The shift from voice to data traffic introduces a new requirement for better performance and high quality of transmission services. Delay, downtime, or performance degradation are not tolerated by real-time and interactive data traffic. Users are more and more dependent on higher speed and multimedia applications. In addition, with the growing number of high speed facilities carrying more traffics and linking large number of users, any network problem will impact an increasing number of users and severely degrade their confidence on the network. Such complex situation requires highly qualified network management experts to appropriately handle the testing management problem. Another motivation of TMN testing is the need for maintenance costs reduction. The need to suppress the risk of network quality degradation is an economic need that focus on the reduction of networks operation costs. There is a considerable pressure and stress on network management personnel to drastically reduce operation center costs.
From the testing perspective, an appropriate solution for the specification, design and implementation of tests management must be worked out with these considerations in mind.

3. TESTS MANAGEMENT IN TELECOMMUNICATION NETWORKS

This section focuses on software testing tools, gives a brief overview of existing testing equipment and draw a picture of current telecommunication network testing.

3.1 What is to be managed ?

The environment to be considered while addressing the telecommunication network management testing is composed of: (i) the customers/users of services provided by these networks, (ii) the operators/owners of the networks, (iii) the managed telecommunication networks.
From a management perspective, the customers and users of the networks services are viewed as human monitors of managed system they use. The information they provide

when notifying any abnormal conditions that affect the services is useful for management purposes. Another important issue to be considered is the organizational policies defined by the owners of the managed telecommunication networks. They intervene at a higher level of the management by ensuring the application of policies they defined to preserve a high quality of the network and the services provided to their customers. Finally the managed telecommunication network is the main component of the management environment to be controlled from several perspectives.

The telecommunication network example presented in Figure 4 depicts a generic network. A typical telecommunication network is composed of terminating points connected by physical paths (link), multiplexor equipment or digital cross connect system (DCS). Several circuits (voices and data) are multiplexed onto smaller number of higher speed circuits carrying data between multiplexers. These circuits are composed of sequences of physical connection links (e.g., cables, fiber, wireless links) and number of equipment (e.g., CSU, DACS, NUI, Repeaters).

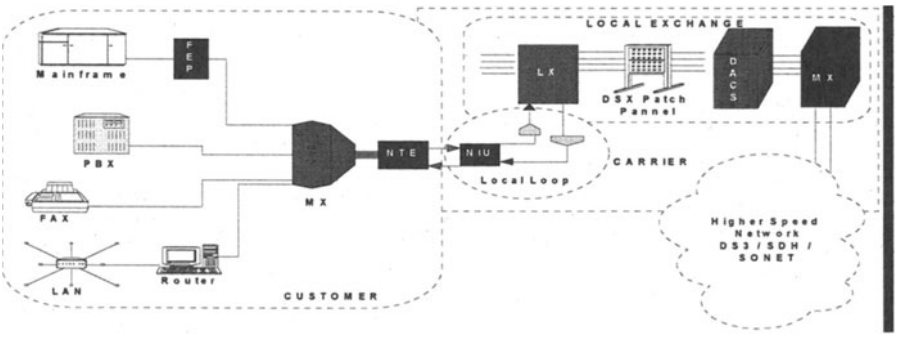

Figure 4 : Example of Managed Telecommunication Network

The description criteria of the presented network is based on ownership (i.e., customer network part local loop, and carrier network). The customer part of the network contains multiplexing system used to feed into the carrier's network customer applications. All type of traffic like voice, data, video, and fax are multiplexed and carrier by higher speed networks. The customer network incorporates: mainframe, LAN, PBX, Fax, stand alone PCs and terminals. It also incorporates interconnection components such as Gateways, Routers, and Network Terminating Equipment (NTE). Some of these managed elements have some management capabilities. For example, added to its basic function (e.g., electric isolation between the network and the customer equipment), NTE is capable of monitoring telecommunication access point (e.g., E1 access point), to provide testing facility (e.g., loop back for bit error rate testing), and to generate alarms (e.g., AIS: Alarm Indication Signal). At the local loop, Network Interface Units (NIU) limit the border between the customer network and the carrier network and provide several management capability (e.g., full test access, loop back facility, etc.). Line repeaters are used to regenerate the signal on the loop and also provide loop back and network troubles detection facilities. Finally the carrier domain is composed of local exchange, cross-connect and multiplexing system. The local exchange is composed of office equipment that regenerates multiplexed signal before

their routing. It is also composed of DSX patch panel, or Digital Access Cross-connect (DACS). Data traveling on the networks circuits are monitored, amplified by the intermediate equipment. Telecommunication networks that use Synchronous Digital Hierarchy (SDH) have capability to detect faults on different levels via embedded overhead information such as check sum (CRC-4) and trial labels.

3.2 Telecommunication Networks Tests Management

3.2.1 Tests Units

Number of instruments, devices and equipment explicitly dedicated for the monitoring and testing of network components are widely used in telecommunication network maintenance [12]. We call an entity with testing capabilities a *Testing Unit* (TU). It is used in local management site or remotely. While used remotely it is called *Remote Testing Units* (RTU). A TU is a software tool that remotely control testing equipment or stand alone managed equipment. It has a number of testing capability to be requested directly (on the TU board), or remotely via a control software system.
TUs are classified based on the following criteria : the category of remote control used, the transmission/reception capability, and the type of provided interface.
A TU with generic driver is controlled via a generic driver. Its user interface depends on the technology considered for test (e.g., T1 Bert, E1 Jitter, DS-3 Slip and Wander), but is completely independent of the testing unit. The test unit can have a terminal type control. This type of TU does not have any driver, and can be integrated to test applications in the following manner: associate an address of one of the following type : serial port, modem, X.25 or TCP/IP to the TU and establish automatically an ASCII terminal session (e.g., Telnet service in TCP/IP) between the client and the TU. A TU can have a Windows/DOS, or an X Windows/UNIX type of control. This type of TU is typically a Personal Computer equipped with interface cards that allow to perform network testing. The software that run within the TU which controls its functionality is often a Windows 16 bits software or a UNIX/Xwindows software. Finally an undergoing class of TU is that one with opened type of control. Current development will lead in a near future to a new generation of TUs that are controlled in an opened way. The standard used are CORBA based and ITU-T CMIS/CMIP protocols.
The transmission/reception characteristic of TUs performing tests at physical layer is described in terms of number of transmission/reception ports. A half duplex TU has one transmission port and one reception port, a dual monitor TU has one transmission port and two reception ports, and the full duplex TU has two transmission ports and two reception ports.
The last TU classification criteria is based on type of Interfaces that the unit is able to connect to and perform testing on. TUs have often more than one test interface. Almost all the TUs can use only one of these interfaces during a test session. For example a FIREBERD 6000 which is a TU from Telecommunication Techniques and Corporation (TTC) can in theory be equipped with eight different interfaces such as T1, E1, DS-3, V.35, X.21, 232 TTL. Some TUs such as those from WANDEL & GOLTERMANN (WG) are manufactured with a certain number of interfaces that can never be modified by the user. However other TUs such as FIREBERD can be modified by the user, but

only in a cold manner (i.e. the device must be powered off before the modification). Thus when a software connects on such a device, what is detected will be available for all the duration of the session.

3.2.2 Testing Realities

Telecommunication networks testing activities include : tests configuration (connections, setups), tests scheduling/execution, tests results collection/analysis, and fault isolation. In general manual practices are more frequent in testing. They often lead to human errors and mismatches. Such a testing lack clear documented cases and appropriate guidelines for tests results interpretations/usage. There is no clear test objectives neither good tests classifications. The only available interpretation is that relying on highly experienced and skilled operators. The control of tests is also done manually. Known tests technology are proprietary and depend on vendor, manufacturer, organization policy, or test equipment. The classic manual practices of troubles causes isolation are based on the collection and usage of tests results such as: bit errors, bite error rate (BER), Far end Alarm Signal (FAS) errors, pattern slips, error-free seconds (EFS), percent error-free seconds (%EFS), etc.
Two types of testing are identified : *out-of-service* (OOS) *testing* and *In-Service* (IS) *testing*. The OOS testing is used when installing network components (e.g., T1 Circuits) and verifying end-to-end continuity. It is also used for fault isolation by inserting pseudorandom patterns that simulate a live data exchange and allows to collects tests results to be analyzed for faults isolation. Some acceptance and conformance testing including time and stress tests are also performed while the tested system is out of service. IS testing are performed while the system is on line and is provided the service for which it's tested. The later type of test can be disruptive thus can affect services provided by the managed network.
Basically there is two generic testing configuration approaches: *loopback testing, and end-to-end testing*. Loopback testing is performed with only one TU connected to a element of the network segment to be tested. It is characterized by a limited faults detection capability. For example, while testing a circuit in a loop back configuration, only one direction can be checked. Due to their management capability, most NEs remove code errors they receive (fault tolerance) before transmitting the data. This affect the analysis of results and by the way the faults diagnosis. End to End testing overcome most of the enumerated drawback of loopback testing. It is performed with two TUs located at both sides of the network segment or circuits to be tested. This testing configuration allows analysis in both directions of the segment under test. This approach is better than loopback because the direction of errors may easily and quickly be found.

3.2.3 Specific Test Categories

As X.737 test categories are generic, we refine and specify telecommunication network tests classes [12]. These specific tests classes are :

- ***Continuity Test :*** This test is aimed to show that continuity of bit information transmission will not be corrupted or abnormally delayed on a path between

the TU and a looped-back NE.

- ***Signal Delay Test:*** two types of delay measurements are identified. (1) Equipment Delay Test allows to verify if the delay time between the receipt of an information bit and the retransmission of the same bit on any channel of the NE shall not exceed a given tresholded value (0.5ms). (2) Path Delay Test allows to verify if the delay time between the receipt of an information bit and the retransmission of the same bit on any channel of the transmission path shall not exceed Xms. It shows that the signal delay on a looped-back transmission path is less than Xms (X=60ms for FO, and X=600ms for Satellite).
- ***Bit Error performance Test:*** this type of test is used to verify that a NE does not introduce bit errors into any channel at a rate greater than 1 in 10^{10} for any equipment configuration when measured for 24 hours. A bit error is defined as any output bit which does not have the same logic state as the corresponding input bit. The objective of this test is to show that the tested circuit will introduce no more than 1 bit error on any channel over a 24 hours interval.
- ***Jitter Measurement Test:*** three type of jitters measurements are described. (1) Input Jitters tolerance Test consists in identifying the maximum allowable number of jitters generated by a NE without any incrementation of bit error. (2) Allowed Output Jitter Test shows a NE Jitter value is not greater than that specified by CCITT Recommendations (G.743 for T1 1.544 kb/s interfaces and G.703 for E1 2.048 kb/s interfaces). With no jitters at the input to the multiplexer and demultiplexer, the Jitter at the demultiplexer output should not exceed 1/3 unit interval peak-to-peak. The objective of this test is to shows that output from an NE is less than a given limit (1/3 UI for 2.048 kb/s disgroup) when measured at a number of frequencies in a given interval (58 frequencies from 10Mh to 100 MHz). (3) Jitters transfer test consist of the determining at what extent a NE passes Jitter to its output. The objective of this test is to shows how much NE amplifies (or attenuates) jitters present at its input.
- ***VF Tone Generation Test:*** it is an analog continuity like test. It shows that a voice frequency tone can be audibly generated. VF Tone Frequency Response Test is an analog loopback test. It shows that a VF frequency response can be obtained from a loop back.

With this classification and specialization of tests on hand, the remaining question is : what is the distribution and mapping of test classes versus faults classes? The issue here is to be able to appropriately monitor the telecommunication networks in order to detect the impairments and the faults symptoms, then select the appropriate tests types, category/class, or suites that can accurately locate the source of the fault. Another issue is the management of these testing activities that could include more complex problems such as the analysis of alarms and faults symptoms, the collection of test, the storage of tests results and also the automatic interpretation of these results. TMN Testing solution discussed in the next section addresses some of these issues.

4. TOWARD A FULL TMN COMPLIANT TESTS MANAGEMENT

4.1 TMN Current State

Despite the emerging research works and available TMN products [13], several barriers and obstacles are encountered while applying TMN principles. There is a big gap between what TMN standards say and what is currently implemented. TMN tells where to start but never indicates where to stop. This leads to several conflicting interpretations and implementation of standards. As stated before, the first constrains faced by TMN application developers is the huge number of standard documents and the framework complexity and instability. TMN architects also have to handle the full TMN/OSI Protocol stack implementation complexity and high cost. Even thus, existing TMN implementations have several performance problems. Simple Network Management Protocol (SNMP) [10] is the widely used and predominant solution in the market because of its simplicity and it availability. Due to the OSI/TMN protocols complexity and a large availability of SNMP based NEs, TMN visibility is limited. TMN Information models also fail to meet existing and future Operation Administration Maintenance & Provisioning (OAM&P) needs. It is unclear how to apply concepts such as service and business layer management because the Logical Layered Architecture (LLA) is difficult to implement: it is hard to identify the border between layers. Furthermore R&D costs are higher and developers are resisting to shift to TMN solutions. There is a limited time, restricted initiative in product development and delivery putting stress and lot of pressure to researchers and developers. These limitations motivate progressive evolution toward the full TMN compliant management solution.

4.2 TMN requirements for Testing

There is a need for providing infrastructure to globally manage telecommunication networks testing activities from one end to another. This implies several considerations ranging from user/provider, time schedule, to development platforms considerations. Another requirement is related to the need for a high level and generic testing capability and instrumentation features. Practical and easy to implement solutions, flexible and compromising approach that integrate current practices and TMN concepts are needed. If a TMN test environment has to be deployed, it has to provide a global management infrastructure of the testing activities. This would allow to test the complete behavior of the telecommunication networks and systems. The approach must have a simple but powerful tests and test management description and information model detailed enough to be easily implemented in existing platforms. The automatic collection and analysis capabilities of test results is also highly required. Graphical presentation of tested network and also the ongoing testing activities are required. In addition, browsing and visual presentation of testing MIB (Management Information Base) are also required. Support for test data manipulations (export/import) are needed. Facility to monitor and control the test are also required. From simple tests, a test management system environment should be able to allow an easy and/or dynamic extension to complex test without adding too much effort. A hypertext help facility can be useful for training and

online documentation.

4.3 Directions for Intermediate Test Management

The approach taken consist simply to apply progressively TMN approach and principles to the management of tests activities. The solution proposed start while designing the tests management application by a limited compliance with TMN then progressively upgrade the level of compliance to TMN. The following three tables sketch a guideline design approach for the transition from the completely proprietary solution to a full TMN test management system based to the TMN architectures.

Informational and Functional Architecture

Design issues	From	To
Network Element	NE Entity	Managed Object
Reference points (test and tested)	Relation	Exchanged Object
Test Units (software or devices)	TU Entity	Associated Objects
Tests categories	Tables and procedures	Test Object
Test session	Set of Test Entities	Session Object
Management protocols	SNMP, CMOT/L	CMIP
Communication protocol	TCP/IP	OSI Stack
Work Station	Proprietary	Generic GUI

Functional Architecture

Design issues	From	To
Test Management OSF (Conductor)	Function Entity	Manager (Object oriented)
Performance Management OSF	Function Entity	Manager (Object oriented)
Mediation function (Tests Performers)	Function Entity	Agent (Object oriented)
Interfaces between OSFs	Relation	Exchanged Manage Object
Global Management	Centralized	Hierarchical (LLA)

Physical Architecture

Implementation issues	From	To
Test Management Information Base (MIB)	SQL based	Object Oriented
Blocks (WS, OS, NE, MD, QA, DCN)	Proprietary	Standards
Interfaces (F, Q, X)	Proprietary	Standards

4.4 A Hybrid Test Management System

The application of the directions presented in the previous section can lead to an hybrid performance and test management system for telecommunication networks (Figure 5).

The depicted system is developed within the VIVALDI project[1] . It is aimed to automate and integrate current testing techniques using some TMN guidelines. The system is initially developed as a centralized management application (management server) witch implements two Operation Systems Functions: *tests management OSF* and *performances management OSF*. Client application has been developed in the early stage of the project as a demonstration prototype. It provides Work Station facilities (Graphical User Interface) that allow a Human Machine Interaction to access, in a user friendly way, services provided by the tests and performances manager. This management station is designed to run on Windows 95/NT. It is locally or remotely used by human operators to initiate, execute, control and monitor tests operations and access the telecommunication network performance data.

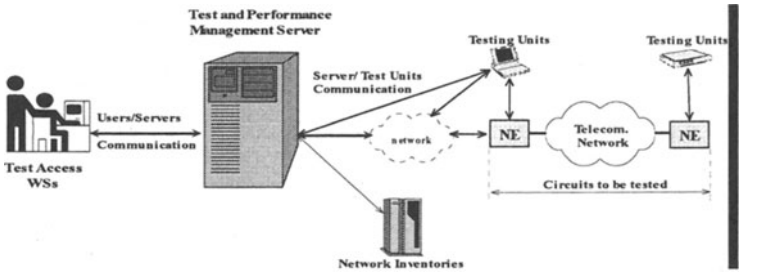

Figure 5 - Simplified Test management Architecture

The management entities have the capacity to access the configuration and inventory database as well as the topology of the managed telecommunication network. The later feature allows to identify the network components to be tested (e.g., circuits relational database) and to provide routing information associated with them. It also provides the available testing and performance measurement resources. The test management system is based on X.745 and X.737 recommendations. Categories of tests defined by X.737 are considered together with the well known tests from telecommunication network people. Specialized Testing Units are connected to the managed network. These TUs are remotely controlled by the tests management server via some «Mediation Devices » not in the sense of TMN. Several tests drivers are defined to allow the use of specialized test equipment provided by different vendors and manufacturers (e.g., FIREBERD 6000 from TTC, PA-41 from WANDEL & GOLTERMNAN, etc.). The performance management performs continual networks polling of telecommunication networks elements using performances monitoring agents that collect performance data. When a control reached by the user threshold is attained, the management system generates alarms and sends them to the central tests and performance management. This module also handles a relational data base (MIB) containing long term (one year) statistical data and information on the performances of network managed elements.

4.5 To a Full TMN Compliance

As we have seen in the previous section, some management components implement

[1] VIVALDI is a project that have been undertaken by ETS (École de Technologie Supérieure) with a subsidy from MINACOM International R&D center.

well defined policies (testing, performance measurements, configurations and planning). To be fully compliant with TMN management solutions must satisfy several constrains. For example, the management information model must be based on standard OSI/TMN recommendations. Communication protocol between TMN entities must ideally be CMIP (Common Management Information Protocol) over which CMIS (Common Management Information Service). Different interactions points defined as TMN reference points between the functional blocks and implemented by various interfaces (e.g., F interface between the management server and the client WS, Q3 interface between the server and the NEs), should also follow TMN recommendations. That is the interfaces should be modeled as objects and communication based on the OSI Stack and CMIP.

Full TMN compliance conditions can be resumed as :

- Specification of an Information model that is independent from technology or vendors (GNIM)
- Clear specification of TMN blocks (WS, OS, MF/QA, NE) with separation of boundaries
- Identification and specification of interfaces (F, Q3, Qx, X, M) using TMN methodology
- Replacement of the ad-hoc communication protocol by CMIP
- Replacement of TCP/IP or Proprietary DCN by OSI Stack
- Development of Q-Adaptors to integrate legacy components
- Migration of the relational or proprietary MIB to an Object Oriented database

5. CONCLUSION

In this paper we have analyzed the conflicting requirements and needs of current telecommunication network testing. The objectif is to provide an appropriate solution to remote testing activities and to automate the procedures. In order to situate the design context, a review of existing TMN principles and framework have been presented. The current telecommunication testing activities with respect to the TMN driven forces were also reviewed. The main test management requirements were analysed and then the problem addressed by this paper: «how to fly toward a Full TMN Distributed Testing Management ?» was discussed. An intermediate solution for the development of a partially centralized test management based on TMN principles was adopted. The requirements for a transition to a full TMN implementation was then discussed. It was then shown that a smooth transition toward a full TMN can efficiently bring the realization of the telecommunication network testing. In order to validate the proposed ideas, a telecommunication network is presented as a case study.

Future work will be directed toward the enhancement of the TMN testing approach, taking into consideration existing testing work such as protocol validation and conformance testing. Furthermore a new implementation solution based on the mobile agents paradigm is under development.

6. REFERENCES

[1] ITU-T Recommendation M.3000, *Overview of TMN Recommendations*, Geneva 1994.

[2] ITU-T Recommendation M.3010, *Principles for a Telecommunications Management Network*, Geneva 1992.

[3] ITU-T Recommendation M.3200, *TMN Management Services : Overview*, Geneva 1992.

[4] ITU-T Recommendation M.3400, *TMN Management Functions*, Geneva 1992.

[6] ITU-T Recommendation M.3100, *Generic Network Information Model*, Geneva 1995.

[7] ITU-T Recommendation X.737, *Test Management Function Management function.*

[8] ITU-T Recommendation X.745, *Diagnostic and Confidence Tests Categories.*

[9] ITU-T Recommendation X.720, *Information Technology - OSI - Structure of Management Information : Management Information Model,* Geneva 1992.

[10] William Stallings, *Networking Standards - A Guide to OSI, ISDN, LAN and MAN Standards*, Addison Wesley Publishers Ltd., 1992.

[11] Roch H. Glitho and Stephen Hayes, *Telecommunications Management Network : Vision vs Reality*, IEEE Communications Magazine, March 1995.

[12] Bellcore, GR-818-CORE, *Network Maintenance : Access and Testing - Generic Test Architecture,* Bell Communication Research, 1995.

[13] Bernard S. Ku, *Use of TMN for SONET/SDH Network Management,* NOMS'96 - IEEE/IFIP 1996 Network Operations and Maintenance, Conference Proceeding, Volume 2, April 1996.

[14] TTC, *Implementing a Distributed Test Solution, Telecommunication Techniques* Corporation, 1996.