INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3013

(02/2000)

SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

Telecommunications management network

Considerations for a telecommunications management network

ITU-T Recommendation M.3013

(Formerly CCITT Recommendation)

ITU-T M-SERIES RECOMMENDATIONS

TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION M.3013

CONSIDERATIONS FOR A TELECOMMUNICATIONS MANAGEMENT NETWORK

Summary

The Telecommunications Management Network (TMN) is implemented to support management activities associated with telecommunication networks. This Recommendation introduces essential considerations needed to support installation and operation of a TMN based on the TMN principles, concepts and architecture, which are described in Recommendation M.3010. Issues associated with evolution of new technologies for TMN applications are also identified.

Background

This Recommendation is based upon material extracted from Recommendation M.3010 (1996). In this Recommendation the material has been updated, refined, and expanded to assist in the planning, design, implementation and operation of a TMN.

Source

ITU-T Recommendation M.3013 was prepared by ITU-T Study Group 4 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on 4 February 2000.

Keywords

Architecture, Implementation guidelines, Telecommunications management network (TMN).

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Recommendation M.3013

CONSIDERATIONS FOR A TELECOMMUNICATIONS MANAGEMENT NETWORK

(Geneva, 2000)

1 Scope

This Recommendation describes how the Telecommunications Management Network (TMN) functional, information and physical architectures, which are defined as frameworks in Recommendation M.3010, can be used to support the requirements, analysis and design efforts necessary to implement TMN(s). This Recommendation provides guideline information that may be useful for TMN designers, architects and implementers. Many issues are enumerated that may be taken into consideration for implementing, upgrading or expanding a TMN capability.

The design of a physical architecture is based upon logical, functional and information architecture specifications. Since multiple physical architectures may meet the requirements of the logical architecture, TMN designers/architects should consider the following in order to achieve an optimal physical architecture design to be implemented:

- determining access and control points with associated interaction models;
- maintaining necessary interfaces to non-TMN systems;
- considering evolution of interface technologies;
- establishing system performance requirements;
- developing system reliability, availability and survivability requirements;
- identifying system administration and other system support requirements.

This Recommendation enumerates a number of considerations (non-exhaustively) in support of designing a physical architecture. This Recommendation also examines emerging technology directions that may support the business requirements of service providers and may also provide support in meeting the needs of the TMN physical architecture design to be implemented.

2 References

2.1 Structure of TMN documentation

Many ITU-T Recommendations apply to TMN applications. This clause identifies the content matter of the various series of Recommendations that relate to TMNs. These Recommendations are continually in the process of expansion and enhancement to fulfil evolving requirements. Refer to current ITU-T catalogues for latest lists of applicable Recommendations.

2.1.1 TMN overview

M.3000.

2.1.2 Architecture

M.301x-series, M.360x-series, M.361x-series, X.70x-series.

2.1.3 Interface specification methodology

M.3020, G.851.x-series.

2.1.4 Management requirements, functions and services

M.32xx-series, M.3300, M.3400, G.784, G.852.x-series, M.36xx-series.

2.1.5 Management information models

M.31xx-series, G.774.x-series, G.85x-series, M.31xx-series, M.364x-series, Q.82x-series, Q.83x-series, Q.853.x-series, Q.854.x-series, Q.855.x-series, X.751.x-series, G.776.x-series.

2.1.6 Communication services and protocols

Q.81x-series, Q.28xx-series, X.71x-series, Q.94x-series, G.773, G.784.

3 Definitions

Definitions of terms are provided in Recommendation M.3010.

4 Abbreviations

This Recommendation uses the following abbreviations:

A	Agent
AD	Adaptation Device
AE	Application Entity
ATM	Asynchronous Transfer Mode
BM	Business Management
BML	Business Management Layer
CCAF	Call Control Access Function
CCF	Call Control Function
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
DAP	Directory Access Protocol
DCF	Data Communication Function
DCN	Data Communication Network
DFP	Distributed Functional Plane
DIB	Directory Information Base
DIT	Directory Information Tree
DN	Distinguished Name
DO	Directory Object
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
ECC	Embedded Control Channel
EM	Element Management
EML	Element Management Layer

EMS	Element Management System
FE	Functional Entity
GDMO	Guidelines for the Definition of Managed Objects
GFP	Global Functional Plane
IETF	Internet Engineering Task Force
IIOP	Internet Inter-Orb Protocol
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IOR	Interoperable Object Reference
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M	Manager
MAF	Management Application Function
MCF	Message Communication Function
MD	Mediation Device
MF	Mediation Function
MIB	Management Information Base
MIT	Management Information Title
MO	Managed Object
NE	Network Element
NEF	Network Element Function
NEL	Network Element Layer
NM	Network Management
NML	Network Management Layer
NSAP	Network Service Access Point
ORB	Object Request Broker
OS	Operations System
OSF	Operations Systems Function
OSI	Open Systems Interconnection
OSIE	Open Systems Interconnection Environment
PE	Physical Entity
PP	Physical Plane
PTO	Public Telecommunication Operator
QA	Q adaptor

QOS	Quality of Service
RDN	Relative Distinguished Name
RFC	Request for Comment
SCEF	Service Creation Environment Function
SCEP	Service Creation Environment Point
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDH	Synchronous Digital Hierarchy
SDP	Service Data Point
SIB	SMDS Interface Protocol
SLA	Service Level Agreement
SM	Service Management
SMAF	Service Management Access Function
SMAP	Service Management Access Point
SMF	Service Management Function
SMK	Shared Management Knowledge
SML	Service Management Layer
SMS	Service Management System
SNMP	Simple Network Management Protocol
SRF	Specialized Resource Function
SS7	Signalling System No. 7
SSF	Service Switching Function
SSP	Service Switching Point
TCP	Transmission Control Protocol
TL1	Transaction Language 1
TMN	Telecommunications Management Network
TMN-AE	TMN-Application Entity
UPT	Universal Personal Telecommunication
VoIP	Voice over Internet Protocol
WSF	WorkStation Function
XA	X Adaptor

5 Conventions

None.

6 General design and implementation considerations

6.1 Introduction

The design and implementation of a TMN system should consider three important architectures:

1) physical;
2) informational; and
3) functional.

These are defined in Recommendation M.3010 and discussed in this Recommendation.

The implementation and design of these architectures in a TMN system fulfil business requirements of an organization. Technologies pertaining to design and implementation should be selected by giving consideration to a business model. Examples of various technologies are presented in this Recommendation. New Recommendations (e.g. functional models and information models) may be developed in the future that support additional business considerations. This clause identifies some architecture aspects that impact the design and implementation of a specific TMN system or component.

6.2 Requirements impacting design and implementation

A TMN design and implementation specification should be given with the minimum number of requirements that convey the needs of business. In the process of specifying functional, informational and physical requirements, consideration should be given to (but not limited to) the following:

- cost of implementation and life-cycle cost;
- selection of a suitable modelling language used to describe requirements, analysis and design. Refer to Recommendation M.3020 for more detailed information;
- specifying exposed functionality and information at the reference points that lead to a physical implementation. These specifications should be based on interaction between application and business models. These application and business models may be based on either new or existing telecommunications or information technology business domains;
- relationships between parties, i.e. interaction models (within a TMN or between TMNs), e.g. between producer and consumer, publisher and subscriber, client and server, peer TMNs, manager and agent, public telecommunication operators (PTOs), etc. An example of interaction is one-to-one (e.g. operations system (OS) with network element (NE), OS-OS, PTO-PTO, peer-to-peer), one-to-many (e.g. OS-multiple NEs), many-to-one (e.g. multiple OS-NE);
- specification of particular interoperability requirements;
- testing of conformance of function blocks with informational and functional requirements at the exposed interfaces or reference points chosen to be points of integration. A function block is the smallest deployable unit of TMN management functionality that is subject to standardization;
- testing of conformance with any mediation requirements to compensate for function blocks that do not support the full scope of the information model;
- testing of conformance to any Q adaptor requirements between the m and q reference points;
- testing of compliance with specified Recommendations, as needed, especially Recommendations Q.811 and Q.812.

6.3 Physical architecture overview

The TMN function blocks defined in the functional architecture described in Recommendation M.3010 may be implemented as physical entities. The TMN physical architecture defines these entities as physical blocks and names the interfaces between them. The physical block should not be interpreted to be a single physical computer system but may be realized as a collection of computer systems interconnected to form a virtual single system, as a single physical computer system or as a distinct application on a software system.

The interfaces are interoperable and defined by a set of protocols, message formats and semantics used to communicate between the physical blocks. The protocol options are documented in Recommendations Q.811 and Q.812. The messages and semantics are determined by standard information models defined to support specific management functionality.

Figure 1 shows an example of a physical architecture. It represents each of the functions as physical blocks and illustrates how a number of interfaces might share communication paths within a given TMN physical architecture.

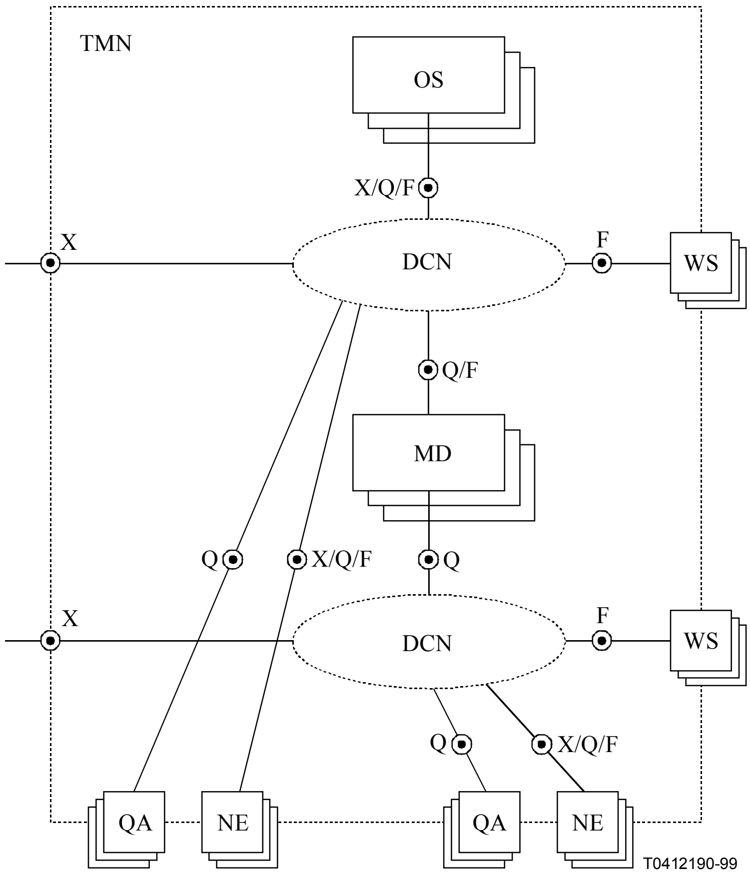


Figure 1/M.3013 – Examples of interfaces for the TMN physical architecture

6.4 Physical block impacts for design and implementation

6.4.1 Network element

Network Elements (NEs) support the deployment of telecommunication services through various network technologies implemented as physical equipment and software. A NE performs the Network Element Function (NEF) and may also perform one or more Operations Systems Functions (OSFs), Transformation Functions (TFs), or workstation functions. The study of various application examples leads to the ability to distinguish among the following functions contained in a NEF:

- telecommunication functions that play a role in providing telecommunication services. Typical functions are switching and transmission;
- telecommunications support functions that do not directly play a direct role in the telecommunication services. Examples are failure localization, billing, protection, switching and air-conditioning.

NEs may be distributed or centralized. Various parts of a NE are not geographically constrained to one physical location. For example, the parts may be distributed along a transmission system. An example of a distributed NE is illustrated in Figure 2.

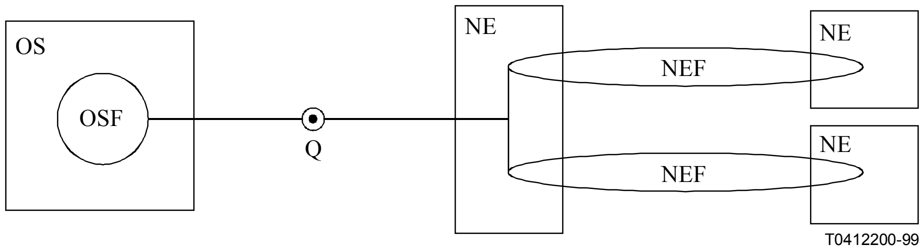


Figure 2/M.3013 – Distributed network element

6.4.2 Operations support system

Operations System (OS) physical architecture must provide the alternatives of either centralizing or distributing the OS functions and data. These include:

- support application programs;
- database functions;
- user terminal support;
- analysis programs;
- data formatting and reporting.

The OS functional architecture may be realized on various numbers of OSs (or MDs, NEs), depending on the network size, functionality required, reliability, etc. The categorizations of TMN protocol selection attributes are also important factors in the OS physical architecture. For example, the choice of hardware depends strongly on whether an OS provides real-time, near real-time, or non-real-time service.

Normally, OS functions will be implemented in a set of OSs with a Q, X, or F interface connected through the DCN. However, this should not preclude a practical realization whereby these functions are implemented in a NE or a MD.

OS Functions (OSFs) enable cost-effective implementations of the connection of NEs of different complexity (e.g. switching equipment and transmission multiplex equipment) to the same OS. In addition, an OSF gives the capability for future design of new equipment to support a greater level of processing within individual NEs, without the need to redesign an existing TMN.

6.4.3 Workstation

Workstations (WSs) allow human operators to view and manipulate objects in the TMN, along with many other capabilities. For purposes of this Recommendation, the WS is considered to be a terminal connected via a DCN to an OS or a device with a Transformation Function (TF). This terminal has sufficient data storage, data processing, and interface support to translate the information between the g reference point and F interface.

A WS that can access TMN physical blocks in more than one TMN is considered to be a part of the particular TMN during the time it is exchanging management information. WS may also have simultaneous access to multiple TMNs.

WS functionality can be distributed, where different parts of the WSF reside on different hardware. For example, detailed layout information (e.g. colours, lines and pixels) can be sent to a terminal by a more powerful managing workstation. In this case, the managing workstation may be thought of as a "display client" that issues requests to update the display, while the terminal may be thought of as a "display server" that responds to these requests. A distributed functional configuration can support greater flexibility for service providers by controlling costs while maximizing productivity.

Figure 3 illustrates the simplest case. The Workstation Function block (WSF) is not distributed, and it is colocated with an OSF in a physical building block, the OS. The f reference point is internal. One piece of processing equipment with built-in graphical display supports the WSF and OSF.

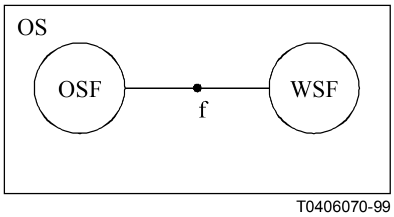


Figure 3/M.3013 – Example WSF in an OS

Figure 4 provides another example where the WSF is not distributed. In this case, the OSF resides in one building block (the OS) and the WSF resides on another (the WS). The f reference point is between these physical blocks and is implemented over an F interface.

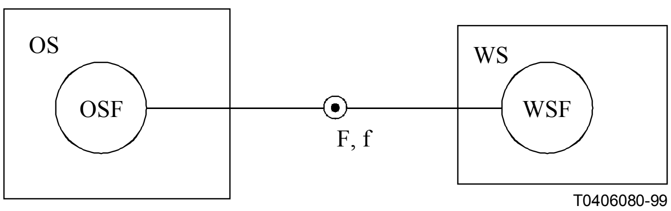


Figure 4/M.3013 – Another example WSF in a WS

Figure 5a provides an example of one way in which the WSF may be distributed, thus creating a distributed implementation of the workstation physical block. In this example, the f reference point is external and implemented over an F interface. The two workstations on the right side may be "display servers", while the "display client" is the WS shown interfacing the OS via the f reference point.

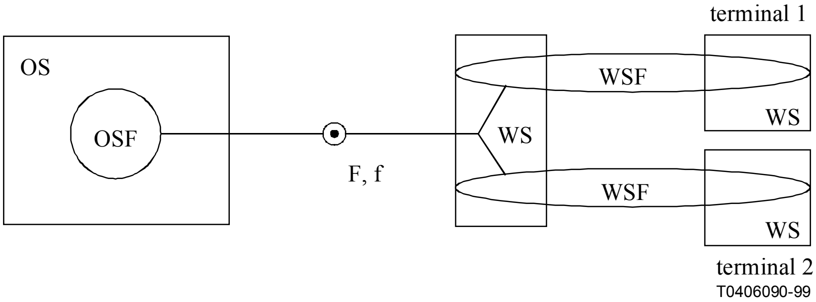


Figure 5a/M.3013 – Example of distributed WSF

Figure 5b shows another example of distributed WSF. In Figure 5b, the OSF and some WSF are colocated on the OS and the f reference point is internal. Some WSF is provided by the display server.

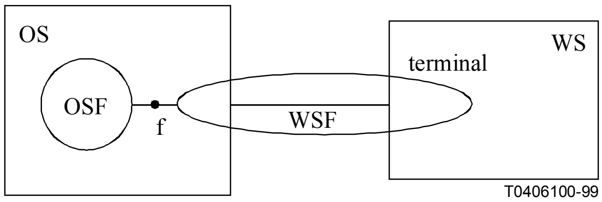


Figure 5b/M.3013 – Example of distributed WSF

Many other configurations of WSF are possible.

6.5 Transformation function considerations

A device that provides a Transformation Function (TF) has been commonly known as a converter or gateway that translates different protocols and data formats for information interchange between physical blocks. More specifically, the mediation device has been defined in the TMN environment as the mechanism that translates between different recognized TMN implementations. An adaptation device, on the other hand, is the mechanism that translates between a recognized TMN implementation and a non-TMN implementation.

6.5.1 Mediation device characteristics

Transformation can be realized in a separate Mediation Device (MD) or shared among NEs. For example, a MD could be used to perform a TF on information passing between a Network Element Function (NEF) and an Operations Systems Function (OSF) in different physical blocks within a TMN. Typically, a MD will fulfil one of two roles. It will provide management functionality to groups of similar network elements (e.g. modems or transmission equipment). It will also provide management functionality to one NE (e.g. digital switch) as shown in Figure 6.

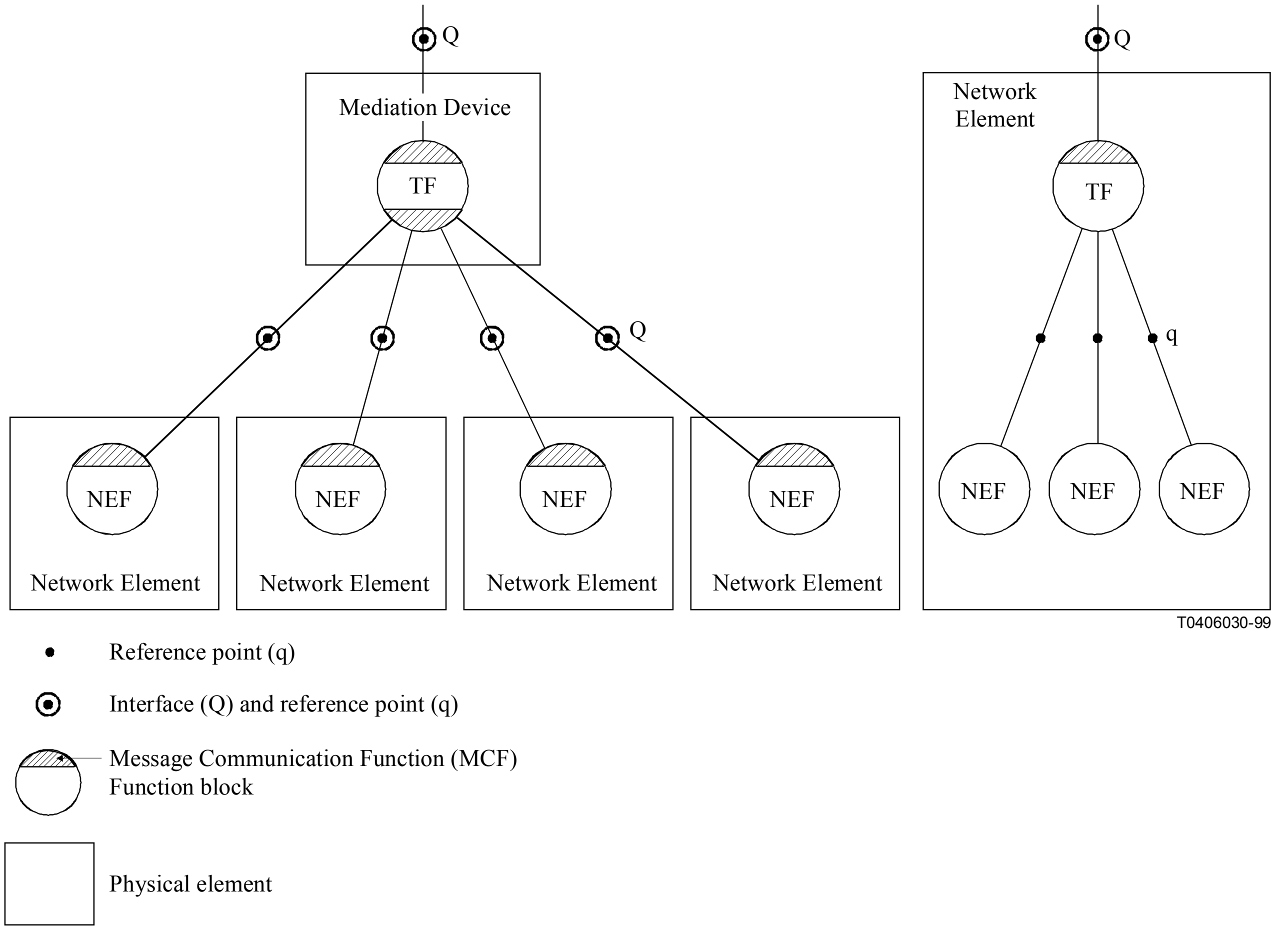


Figure 6/M.3013 – Example of the use of the transformation function

In the example shown in Figure 6, a TF can be implemented as stand-alone equipment as a mediation device or as part of a NE. In either case, the TF remains part of the TMN. In the stand-alone case, the interfaces towards the NEs and OSs are one or more of the standard Q interfaces. TF providing mediation as is part of an NE (e.g. as part of a switching exchange) may also act as mediation for other NEs. In this case, standard Q interfaces to these other NEs are required. The mediation within a NE, which carries out mediation for other NEs, is considered a part of the TMN.

At the service management layer, a MD may also be employed to translate between a physical block using the Common Management Information Protocol (CMIP) with GDMO-defined data and a physical block using CORBA technology. A mediation device can be applied at a Q interface within a TMN or at an X interface between TMNs.

6.5.2 Adaptation device characteristics

Adaptation is a TF used to connect physical blocks providing standard TMN interfaces with physical blocks that do not provide standard TMN interfaces. Adaptation is realized in an adaptation device (AD), which is an adaptor that provides interface conversion. A Q adaptor (QA) applied within a TMN can contain one or more TFs. An X Adaptor (XA) is applied between TMNs and non-TMNs.

An adaptor may also be the means to support other external interfaces, such as simple sensors, indicators, or visible/audible alarms.

6.5.3 Application of mediation and adaptation devices at the Q and X interfaces

In the application of the TF at the Q and X interfaces, Figure 7 presents different configurations for various situations. These situations are described as the following cases in referring to Figure 7:

Case 1 – Between TMN A and TMN B: applies to connecting a TMN with another TMN directly with no protocol or data conversion.

Case 2 – Between TMN B and TMN C: X mediation device applies for connecting a TMN with another TMN.

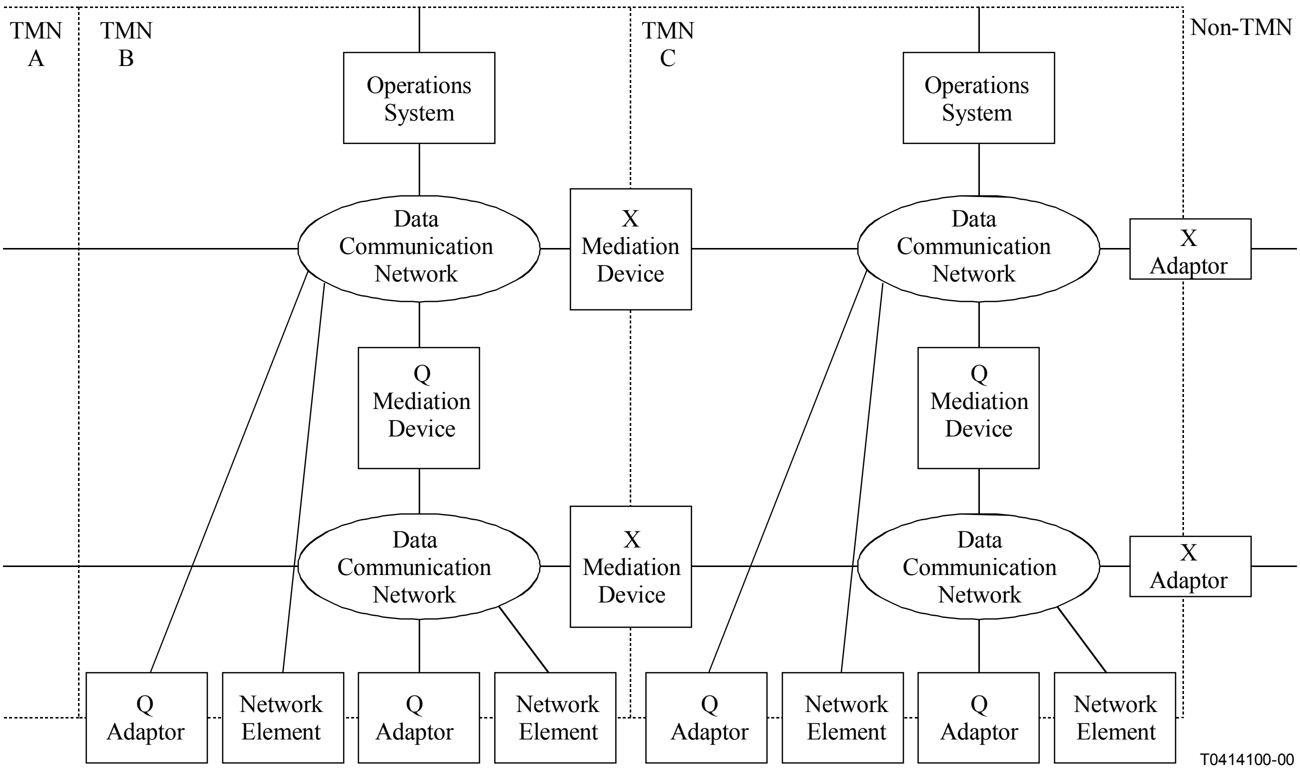


Figure 7/M.3013 – Q and X interface mediation and adaptor cases

Case 3 – On the right side borderline, the X adaptor applies for connecting a TMN with a non-TMN.

Case 4 – Within a TMN: the Q mediation device applies for connecting physical blocks. The major roles of the Q mediation device are:

Case 5 – At the lower boundary of a TMN: the Q adaptor applies for connecting to a non-TMN NE.

Major roles that could be included for adaptation and mediation devices are:

- information translation between different information models using the same TMN protocol;
- protocol conversion between physical blocks;
- data manipulation, e.g. conversion and filtering.

6.6 TMN data communication characteristics

TMN standard interfaces provide for the interconnection of NEs, ADs, OSs, MDs and WSs through the Data Communication Network (DCN). The conceptual DCN is a collection of resources to support the transfer of information among the distributed TMN components. A DCN supports the Data Communication Function (DCF) in a TMN environment. A number of telecommunications technologies can support the DCN functions such as, circuit switching, packet switching, LAN, ATM, SDH and the Internet. Important aspects of the DCN are the quality of service, information transfer rate, and diversity of routing to support specific operational requirements of the TMN.

The goal of an interface specification is to ensure meaningful interchange of data between interconnected devices through a DCN to perform a given TMN function. An interface is designed to ensure independence of the type of device or of the supplier. This requires compatible communication protocols and compatible data representations for the messages, including compatible generic message definitions for TMN management functions. A minimum set of protocol suites that may be applied for transport of information through a DCN can be found in Recommendation Q.811.

Consideration of interfaces should be given to compatibility with the most efficient data transport facilities available to each individual network element [e.g. leased circuits, circuit-switched connections, packet-switched connections (Recommendation X.25), Signalling System No. 7, Embedded Communications Channels of the SDH and ISDN access network D- and B-channels]. If a physical block on one side of the interface supports a different transport mechanism, a transformation function in the form of a Mediation Device (MD) or Adaptation Device (AD) needs to be employed to ensure compatibility of information interchange through the DCN.

NEs, ADs, OSs, MDs and WSs may have other interfaces in addition to the Q, F and X interfaces defined in this Recommendation. These physical blocks may also have other functionality associated with information sent or received via Q, F and X interfaces. Any additional interfaces and related functionality are outside of the TMN.

6.6.1 Messaging availability/reliability

The TMN should be designed to prevent a single fault from making the transfer of critical management messages impossible. Measures should also be taken to ensure that congestion in the DCN does not cause the blocking or excessive delay of network management messages that are intended to correct a failure or fault. For critical communications environments, the interchange of TMN data should be over facilities that are separate from the primary infrastructure of the managed network.

As an example of the single fault situation in a critical NE such as a local switch, a separate and independent channel can be provided for emergency actions to be communicated. An emergency action function can be provided through an independent maintenance capability when the normal OS becomes inoperative or when a NE degrades to the point where the normal surveillance functions cannot operate. For these reasons, an emergency action OS would be separate from the normal maintenance OS, although they are usually at the same location. OSs and NEs that provide an emergency action function may require alternate or duplicate access channels to the DCN for redundancy.

Another example of a critical management operation is accumulation and accounting of charges to the customers. The OSs and the NEs associated with this function may require alternate DCN channels to provide sufficiently high reliability for the process of OSs collecting charging messages from the NEs.

6.6.2 Data communication network considerations

A DCN supporting a TMN has traditionally conformed to the network service of the OSI reference model for ITU-T applications as specified in Recommendation X.200. ITU-T Recommendation X.25 has been a commonly used packet protocol. However, the evolution of telecommunication services is merging circuit-switched and packet-switched modes with advancing technologies of ISDN, ATM, SDH, and the Internet. A variety of telecommunications services can be employed as long as integrity of information transfer can be preserved.

Within a TMN, the necessary physical connection, such as circuit-switched or packet-switched, may be offered by communication paths constructed with various network components, including dedicated lines, X.25 packet-switched data network, ISDN, common channel signalling network, public-switched telephone network, local area networks, terminal controllers, etc. The facilities can be either dedicated to a DCN or shared resources (for example, using SS7 or an existing X.25 or IP-based packet-switched network).

Equipment supporting an OSF must provide for two modes of data communication. These are spontaneous transmission of messages (e.g. for the NEF to the OSF) and a two-way dialogue (e.g. as the OSF obtains supporting information from the NEF and sends commands to the NEF or transfer messages to or from another OSF). In addition, an OSF is responsible for assuring the integrity of the data channels through a DCN. Physical connectivity in a local environment may be provided by a variety of subnetwork configurations including point-to-point, star, bus or ring.

6.6.3 Message communication functionality

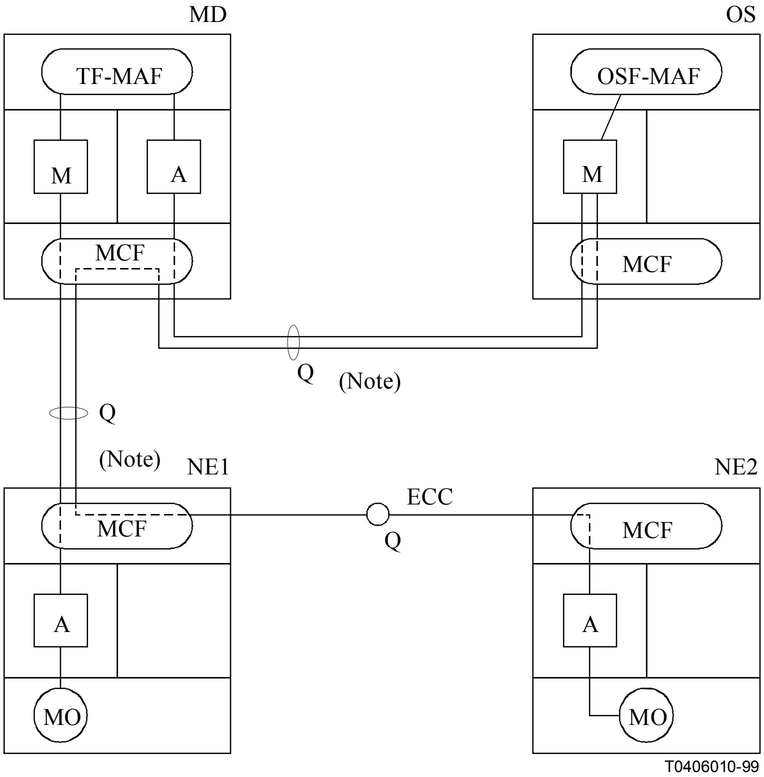
Within a TMN, the communications functions such as information interchange and communications relay functions are performed by the Message Communication Functionality (MCF), which is a protocol generator for information interchange and provides the Data Communication Function (DCF). The MCF interfaces all function blocks in different equipment and consists of one or more of the following processes:

- Communications control:
  - polling;
  - addressing;
  - communications networking;
  - ensuring integrity of data flows.
- Protocol conversion.
- Communications of primitive functions:
  - command/response statement;
  - alarm statements;
  - alarm forwarding;
  - test results/data;
  - operational measurement data;
  - upload of status report;
  - local alarming.

6.6.4 MCF considerations

The MCF allows managers or agents to interwork across the DCN in support of management functionality, which is identified as Management Application Functionality (MAF). When there are instances of different types of DCNs, the use of two MCFs within one device (e.g. MD, NE, OS or AD) may be necessary to allow protocol conversion. TMN protocols supporting the MCF are specified in Recommendation Q.811.

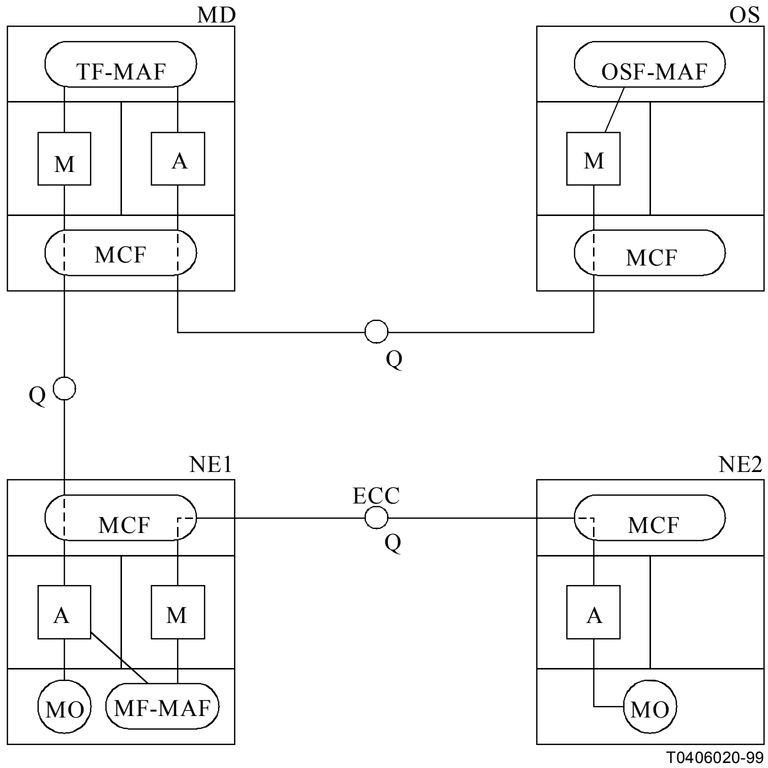
Figures 8 and 9 show examples of how various MCFs are used in various physical devices to provide a Data Communication Function (DCF) in an SDH environment.



A	Agent
ECC	Embedded control channel
M	Manager
MCF	Message communication function
MD	Mediation device
MO	Managed object
NE	Network element
OS	Operations system
OSF-MAF	OS function – Management application functionality
TF-MAF	Transformation function – Management application functionality

NOTE – Indicates both interfaces are in the same transport.

Figure 8/M.3013 – SDH management example (1)



A	Agent
ECC	Embedded control channel
M	Manager
MCF	Message communication function
MD	Mediation device
MO	Managed object
NE	Network element
OS	Operations system
OSF-MAF	OS function – Management application functionality
TF-MAF	Transformation function – Management application functionality

Figure 9/M.3013 – SDH management example (2)

6.7 Interface impacts for design and implementation

6.7.1 OS-NE Q interface

6.7.1.1 Design considerations

The OS-NE interface is positioned at a q reference point in the TMN architecture and can be exposed as a Q interface. An OS at this point in a TMN may perform the element manager function to manage one or more NEs as separate network elements, or in addition it may manage the network elements as a subnetwork and manage the relationship between the NEs.

If the NE and OS support different standard Q interfaces, a mediation device will be required to translate between the two. If the NE does not support a TMN standard interface, i.e. it is outside the TMN, it can be managed by the OS via a Q adaptor. Specific considerations for views of management direction through reference points are presented in 7.3.

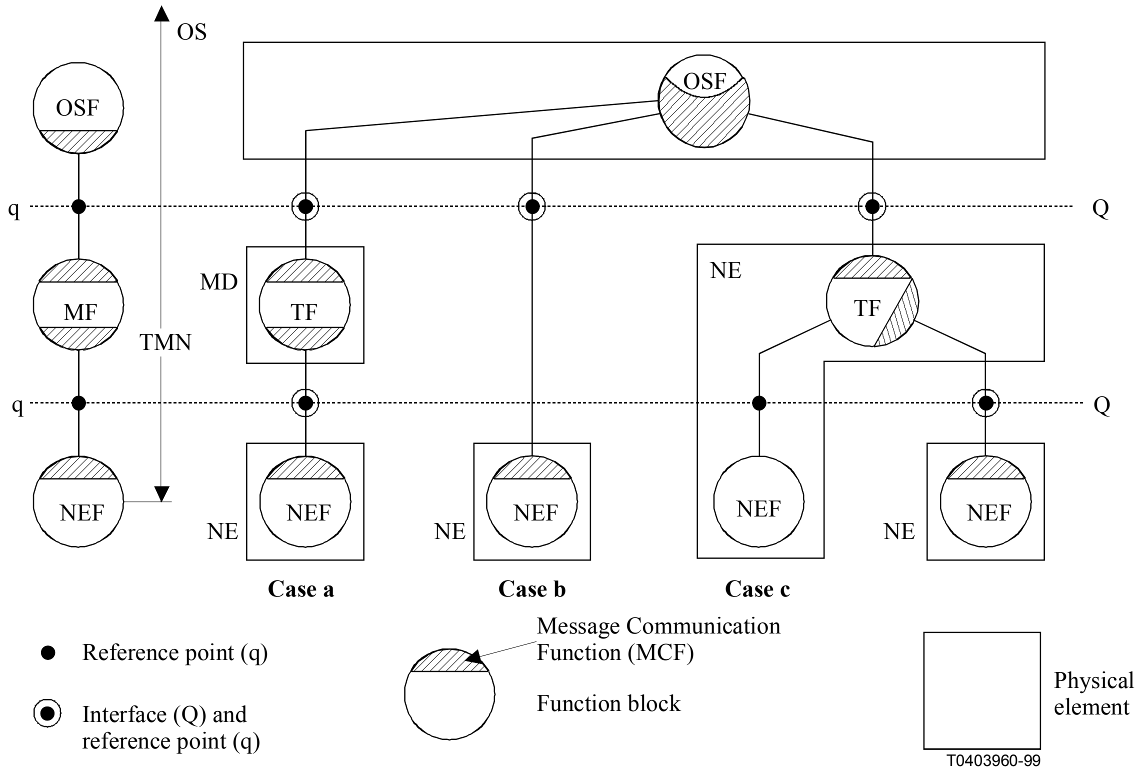
6.7.1.2 Implementation considerations

Figure 10 shows examples of the relationship of the physical configurations to the reference configuration, with the Data Communication Functions (DCFs) not explicitly shown. It illustrates combinations of physical interfaces at the q reference points. At reference points where a physical interface appears, they are denoted with a capital Q.

Figure 10, case a shows an NE connected via a Q interface to an external MD that supplies the TF necessary to convert this interface to the Q interface required by the OS that manages the NE.

Figure 10, case b shows an NE physically connected to an OS via a Q interface.

Figure 10, case c shows an NE with an internal TF that is interconnected to an OSF via a Q interface (see also notes to the figure). An external NE is also connected to this NE via a Q interface.



NOTE 1 – Where only a reference point is shown in the physical portion of this figure, the meaning is that the point is inside a physical box. The designer is free to apply implementation. It is not necessary that this point is physically present inside the equipment.

NOTE 2 – Other equipment, which is necessary for the connection, may be present between two adjacent boxes. This is necessary for the connection of these boxes. The equipment represents the DCF. Such equipment performs OSI network functions and is not shown in this figure, e.g. the Q interface normally connects to the DCN, which provides the data communication to the OS.

NOTE 3 – MCF is only associated with function blocks that communicate over a standard interface. As shown in this figure, communication between function blocks within a box is not supported by MCF.

NOTE 4 – Additional examples showing other physical configurations to manage specific technology are given in clause 7.

Figure 10/M.3013 – Example of the relationship of the physical configuration to the reference configuration (with implicit DCF)

6.7.2 OS-OS Q interface

6.7.2.1 Design considerations

OS-OS interfaces are positioned at q reference points in the TMN architecture and can be exposed as Q interfaces. Various OSs communicate management information in a managed/manager role or in a peer-to-peer role. The transformation function (TF) is needed via an adaptation device (AD) or mediation device (MD) if an OS must communicate over either a non-standard TMN interface or a different standard TMN Q interface.

6.7.2.2 Implementation considerations

Interactions between OSFs within a TMN take place at the q reference points. These interactions may take place between OSFs within a management layer, between adjacent management layers, and across a span of management layers. Specific considerations for views of management direction through reference points are presented in 7.3. See Figure 11.

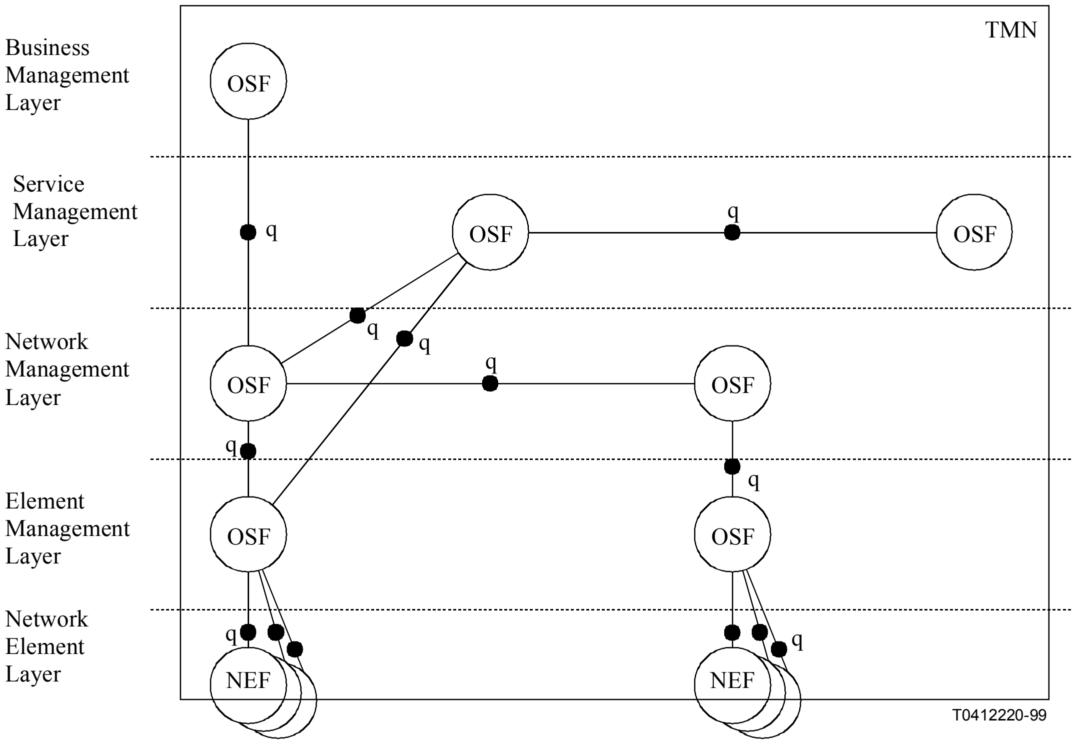


Figure 11/M.3013 – Examples of intra-TMN interactions

6.7.3 OS-OS X interface

6.7.3.1 Design considerations

The TMN X interface specification must cater for TMNs interworking in support of both inter-administrative applications and commercial services. Administratively, the X interface may vary depending upon geographical or jurisdictional boundaries as follows:

- intra-PTOs;
- intra-national;
- international.

There may be protocols and information models to support the X interface that are different, or in addition to, those that support the Q or F interface. Details of X interface protocols are given in Recommendations Q.811 and Q.812.

TMN hierarchies may interact for many reasons including the following:

- to manage the interactions required to provide value-added services;
- to manage a number of geographical/functional TMNs as a single TMN;
- to provide end-to-end circuit/services provision.

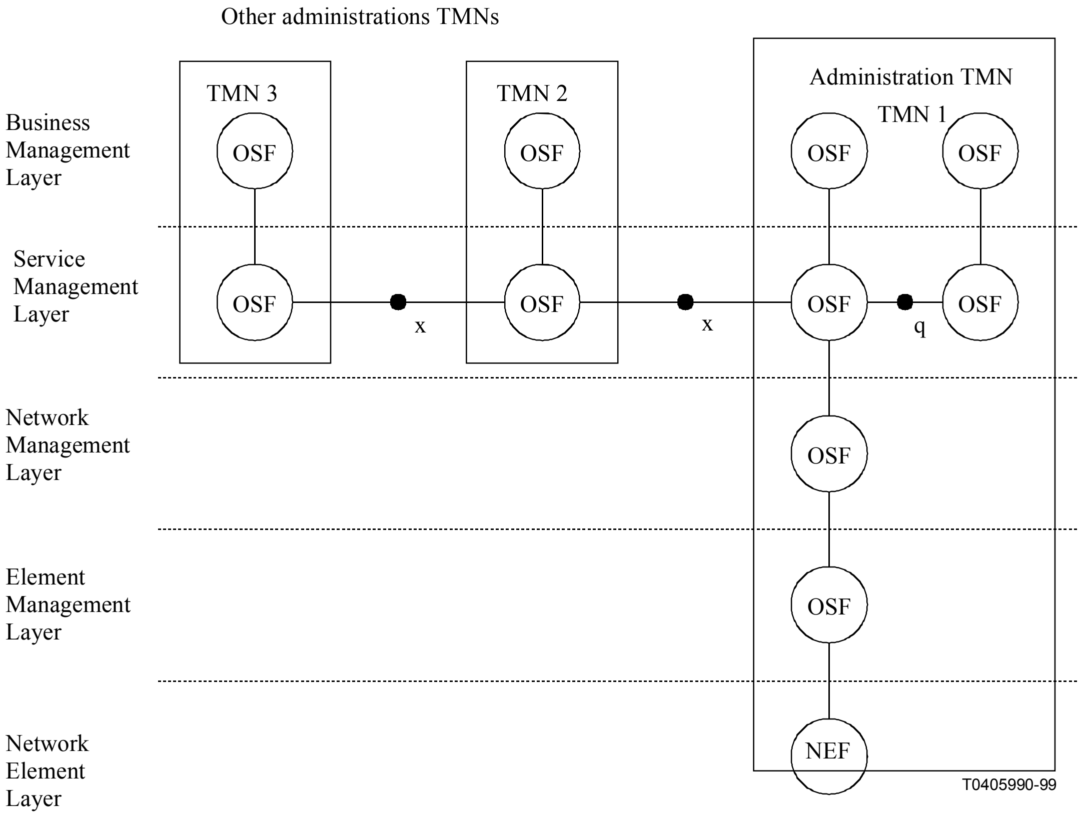


Figure 12/M.3013 – Examples of TMN interactions

One example of TMN interactions at the service management layer between both external and internal organizations is shown in Figure 12. Here, the PTO's TMN (TMN 1) can be seen to support interactions between OSFs within itself via a q reference point and if exposed, a Q interface. However, when an OSF in either TMN 1, 2, or 3 interacts with an OSF in another TMN, this interaction is at an x reference point, which is exposed as an X interface. Note that while all the interactions in Figure 12 are shown between OSFs in the service management layer, interactions may occur at an x or q reference point at layers (exposed as an X or Q interface, as appropriate) other than the service management layer.

Figure 13 shows another possible inter-TMN OSF connectivity example within the management hierarchy. The X interface is most commonly applied to inter-TMN interactions within the service management layer. Interactions between OSFs in other layers are also possible as well as interactions across layers as shown in Figure 13.

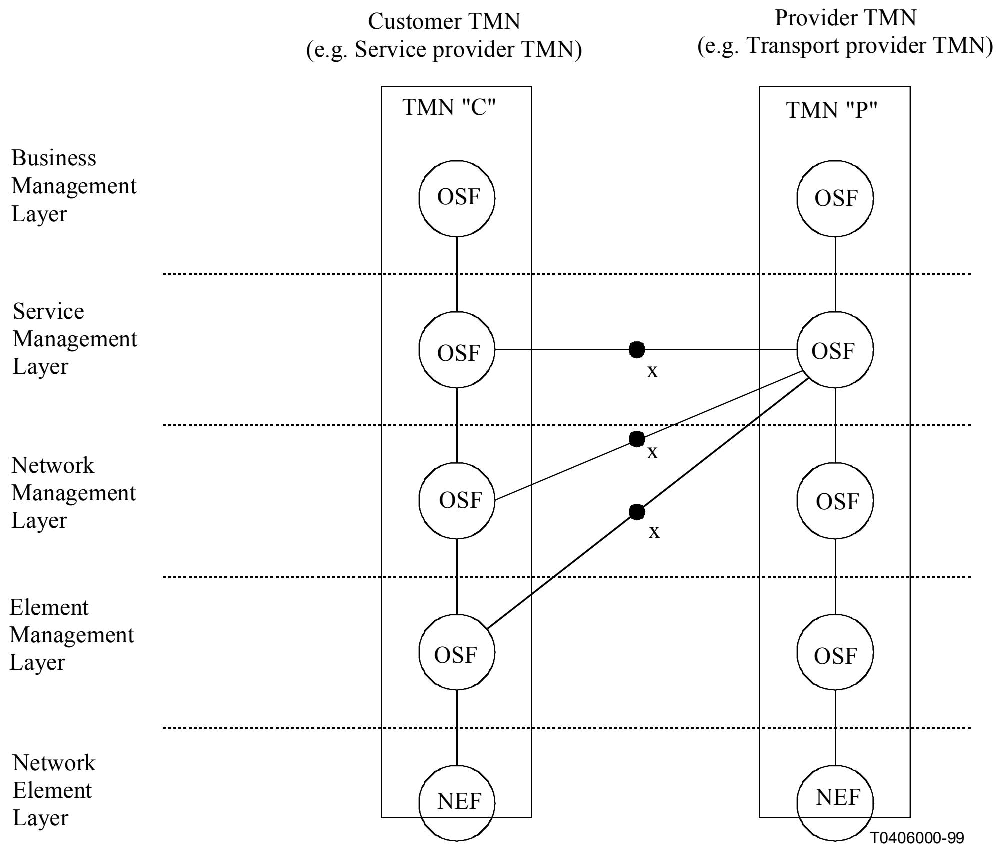


Figure 13/M.3013 – Examples of inter-TMN functional connectivity

In Figure 13, TMN C is an example of a service provider's customer. TMN P is an example of a service provider. For some telecommunications services, the telecommunications services may be delivered to another service provider (TMN C from a transport provider having TMN P). Therefore, TMN C and TMN P may need to interact for the purpose of managing the telecommunications services.

6.7.3.2 Implementation considerations

In the general case of a customer TMN and a provider TMN interaction, the x reference points exposed as an interface between the two TMN OSFs interconnect the provider's service management layer OSF and any management layer OSFs of the customer TMN according to the needs of the customer. Specific considerations for views of management direction through reference points are presented in 7.3.

Like the Q interface, the X interfaces at different layers in the TMN hierarchy have different requirements. However the X interface has stricter security requirements because it sits between PTOs, or service providers. Because the requirements differ at different layers, and as new technologies mature, additional interface technologies may emerge.

When the TMNs support different TMN protocols or information formats, a transformation function is required that is implemented in a MD referred to as a gateway, which sits between the TMNs.

It may also be necessary for TMN systems to exchange management information with non-TMN systems. In this case, a Q adaptor implements the transformation function that provides the gateway between the systems.

6.7.4 OS-WS F interface

6.7.4.1 Design considerations

Workstations provide the user with input, output and edit facilities to enter, display and modify details about objects. This removes the need for an OSF or TF to be knowledgeable about the display capabilities of the user's terminal. The human-machine interface (G interface), be it command line, menu driven, or window based, is supported by the workstation. It is independent of the other TMN blocks and therefore not visible to the F interface.

The information coming over the F interface does not imply its usage at the G interface. At the F interface, a given message or transaction may involve:

- all data needed for one screen picture (graphic and/or text);
- only parts of the data needed for one screen picture;
- data that may result in several screen pictures;
- data that only partly or indirectly appear in screen pictures.

The workstation receives such data and partitions it as needed to support the resulting screen pictures. Data may be communicated synchronously, for example, for on-line transaction processing, or asynchronously, for example, notifications. The following are examples of data categories exchanged in either direction across the F interface:

- security information;
- information pertinent to managed object information (such as alarm indications);
- display support information (such as background maps);
- database queries and results;
- data describing function or command initiation:
  - application commands;
  - system commands (for example, backup);
  - request for command replay;
- data describing function or command responses:
  - messages (information, warning, error);
  - data output as a result of a command;
  - command histories;
- help text.

6.7.4.2 Implementation considerations

There may be protocols to support F interfaces that are different than, or in addition to, those that support the Q or X interfaces. These differences may be related to:

- making communication efficient for the WSs by using formats native to, or easy to support;
- the need to support less-capable WSs such as low-end laptop computers, for example, used to log in from a remote location under extreme low-bandwidth conditions;
- the demands of distributing data updates to multiple WSs simultaneously;
- security issues.

6.7.5 Human-computer interface (g reference point)

The G interface is not currently a subject for standardization within the TMN. However, the standardization of the G interface is currently under study by ITU-T. The following subclauses provide design and implementation considerations for the human-computer interface.

6.7.5.1 Design considerations

The interfaces between WSs and human users are positioned at g reference points. Human users use WSs to communicate with the TMN.

Information is carried over the F interface to support the user at the G interface, but the way the information is viewed differs between these two interfaces. To the F interface, a background map image and an alarm notification are both just data. The user at the G interface sees an alarm event, and the map is just a context to facilitate the user's noticing and identifying the alarm information. Similarly, security information is needed to accompany messages across the F interface but the user at the G interface does not see it (or care).

The majority of the requirements at the F interface (Recommendation M.3300) are present because of the needs of the human user at the G interface.

6.7.5.2 Implementation considerations

Implementation of the G interface is not constrained by this Recommendation. However, PTOs will want TMN interfaces that are easy to learn, remember, use, as well as reduce the frequency and severity of human errors, and are easy to maintain.

There are many different specific G interface instantiations – for different TMN management tasks, different job functions, different organizational schemes. But the needs of PTOs will best be met if some level of standardization is followed: consistent presentation rules, commands, graphical indicators, controls, the use of colour coding, and so on. Degrees of standardization are available by following human factors design guidelines (both those in Recommendation Z.361 as well as those published by the human-computer interaction community at large), standards produced by regional bodies, and standards produced by individual companies to meet their particular business requirements.

6.8 Support functionality

For related technologies providing support functionality for naming/directory services, see 7.5.

7 Additional design and implementation considerations for technology selection and integration

A TMN and its implementation must support the business requirements of the service provider deploying the TMN. This clause discusses the business requirements that are driving the need for technology independence in TMN implementations. Technology independence, however, still requires direction.

This clause also discusses various criteria that may apply to different types of interfaces, which may be exposed within the TMN implementation. These types of interfaces are categorized according to the characteristics of the reference points that are mapped to the exposed interfaces. The reference point concept provides the connection between the TMN functional and information architecture and the TMN physical architecture. (See Recommendation M.3010, Principles for a TMN.)

As noted in clause 9/M.3010, m reference points imply an M interface to an adaptor and the existence of a g reference point may imply a G interface to a WS. Since such interfaces are beyond the scope of this Recommendation, they are not explicitly defined or discussed in this clause.

7.1 Business requirements for technology selection

As the industry faces a growing demand for integrated telecommunications and information system services as well as fast-paced emerging transport technologies, the network management infrastructure developed has to be technology independent. This will enable flexibility in choice of implementing technology and provide an evolving technology base.

This subclause highlights the business requirements that demand a technology-independent network management framework and the approach adopted in this Recommendation to answer those requirements; it also serves as a guiding principle for other TMN Recommendations being developed.

Table 1/M.3013 – Business requirements for technology selection

Business requirements	TMN strategy
An infrastructure that allows faster time-to-market of new services and new products to compete.	• Develop Recommendations that select the appropriate communication technology(ies) that matches business needs. • Maintain a mechanism to manage the evolution of TMN from one technology base to another. • Reuse existing resources.
Robust service and business management capabilities become the key differentiators among service providers. The ability to provide integrated telecom and information technology services is also the key to success.	• Recognize that TMN solutions can become less telecom specific and more information technology specific at higher layers of the TMN architecture. • Utilize technologies that permit the widest use of available domain expertise and internal company resources. Incorporate appropriate commercial technologies, such as those found in the Information Technology (IT) industry. Use IT industry products with IT industry volume pricing, thus improving cost-performance of TMN solutions.
The cost for developing and maintaining an OS must be minimized.	• The inclusion of prominent and available technologies such as distributed processing in the TMN architecture. • Encourage a greater range of domain experts to participate in technology-neutral phases of specifying TMN requirements. • Use software technologies that are widely available in the other industries. • Increase the availability of TMN developers and lowers training costs. • Allow rapid introduction and implementation of TMN applications immediately after requirements and modelling phases through reuse of code or applications in existing service provider systems.

Table 1/M.3013 – Business requirements for technology selection *(concluded)*

Business requirements	TMN strategy
The OS must be able to interoperate in a heterogeneous environment to survive in the global market and business dynamics.	• Provide solutions that reflect needs of participating PTOs. • Choose interface technologies that permit interoperability at the service level among multiple PTOs in a global network. • Choose interface technologies that permit legacy environments to converge with mainstream network management strategies.
Requires an OS phasing strategy for new/start-up operators.	Start with critical operations systems that provide minimum functions to operate the business, and expand the operations systems to include all the TMN functions recommended in the TMN architecture. The OS phasing strategy also depends on the operations processes and the operations budget. The following is an example phasing strategy for a new/start-up operators: • Phase 1: billing and provisioning systems. • Phase 2: maintenance and network traffic management systems. • Phase 3: customer care and integration systems.
Requires a strategy for dealing with legacy systems.	Possible approaches could include: • wrapping legacy systems with appropriate access methodology; • cap legacy systems with adaptors and move new OSs to new technology choices as appropriate; • replace legacy OSs with new OSs implemented with new technologies.

These changing business-driven environments are reflected in new TMN requirements, especially at the higher layers of the TMN, that is at the service and business management layers. These requirements show the need to include incumbent technology available from industries other than telecommunications, such as the mainstream information technology (IT) industry. At these higher layers of the TMN applications often become more business process oriented than telecommunications oriented. To the extent that business drivers and processes influence telecommunications solutions at these layers, technology choices for implementing a TMN are influenced accordingly. Thus prominent and available technologies, such as distributed processing, are included in the TMN architecture.

Additional levels of requirements for new technologies in TMN are needed to support customer service scenarios. The interoperation of systems in a multi-vendor environment is needed to deliver information flow-through. Because no single software interface technology provides all of the solutions, different technologies must be used in combination to provide the anticipated levels of quality for customer service. It is at the higher layers of the TMN where there is the greatest opportunity to provide the maximum integration of service related features that are felt directly by the service customer.

7.2 Considerations for the selection of communication technologies

When selecting communications technologies for interoperability between TMN physical blocks (for both communications within a TMN and communications between TMNs), additional criteria should be considered as requirements on the communications technology selections. All fitness-for-use criteria should be considered in relation to cost where cost can be measured in time, money, or staff. For example, these criteria will lead to technology choices that are optimal to meet business needs. A non-exhaustive list of criteria is provided below.

7.2.1 Criteria associated with functional/information architecture design that may impact interoperability

- user access: technicians, end customers;
- continued use of legacy systems;
- designing reusable components: object-oriented design;
- information architecture details:
  - data stewardship;
  - distributed transactions;
  - database design: queries, data retrieval efficiency, concurrency, threading, caching;
- data synchronization;
- functionality for the job: "best" technology may be the one that gets the job done and is most widely supported by applications. For example, not all interfaces will require scoping and filtering, or event handling.

7.2.2 Criteria based on interface-technology performance

- management request frequency;
- response time: request … to … response;
- prioritization of management operations;
- software upgrade considerations: versioning issues, release dependencies;
- interworking with legacy interfaces;
- reliability, availability, survivability of systems and communications: recovery from failure with associated time, resynchronization of data, load balancing, standby and or duplicate system configurations, systems geographical diversity, access control security issues;
- protocol message formatting: efficient, non-redundant, regular structure;
- ability to handle large amounts of event (asynchronous message) data in real time;
- scoping and filtering capabilities.

7.2.3 Other fitness-for-use criteria for interface technology

- Scalability: from small to large.
- Granularity: resource resolution.
- Portability: development and runtime hardware and middleware environments.
- Security: encryption, non-repudiation, data integrity, access.
- Flexibility: data type flexibility (allomorphism).
- Complexity: number of features implemented.
- Ubiquity: size and distribution of user base.
- Ease of use by programmers: related to ubiquity.
- Modularity: decomposition into building blocks.

7.3 Characteristics of TMN reference points and interfaces

A single TMN functional and information architecture design may be deployed in many different physical implementations, since criteria beyond TMN management services offered with associated management information will determine implementation directions. A non-exhaustive list of these criteria is discussed in 7.2.

Even with this multiplicity of implementation direction, not all possible reference points in the TMN architecture (intra-TMN) will be exposed as standard interfaces for interoperability. Selected interfaces will be those that are viewed as important for a PTO's TMN. Reference points mapped to these chosen interfaces should carefully identify the interacting TMN logical layers, management services offered, and appropriate information view considerations. The information views are realized in standardized protocol-independent information models. The interaction model between function blocks at a reference point (as discussed in 10.2/M.3010) defines function blocks in a managing and managed role with respect to information exchange at a reference point.

Any reference point suitable for exposure as an interface has a characteristic view based upon the logical layer of the managed role. For example, this allows an interaction between an NEL function block in the managed role with an EML function block or NML function block in the managing role to be equivalent.

7.3.1 Characteristics of intra-TMN reference points and interfaces

The TMN logical layer architecture suggests different information views that can be made visible at q reference points.[1] These views are:

- NE view;
- EM view;
- NM view;
- SM view;
- BM view.

Figure 14 illustrates function block interactions between managed and managing roles. The shaded circle represents the primary source of information.

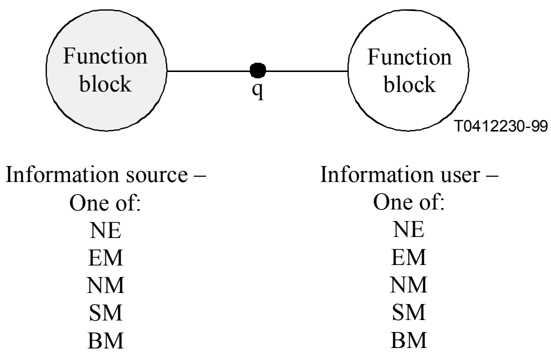


Figure 14/M.3013 – Function block interaction

[1] Requirements and characteristics of the F interface can be found in Recommendation M.3300, F Interface Requirements. F interface characteristics are also discussed in clause 6.

7.3.1.1 Characteristics of the NE view

The NE view may be described by the need for some of the following example characteristics:

- little or no holding time for events (e.g. data must be delivered in real time);
- rapid and high-volume transmission of event messages;
- considerations for archiving and retrieval potentially large amounts of data;
- rapid and multiple database management activities to potentially large numbers of data elements representing managed resources within the NE's internal database;
- rapid and multiple database management activities to potentially large numbers of data elements representing managed resources within the NE's internal database where multiple data elements can be impacted on a single request;
- rapid and multiple status updates of individual managed resources;
- test access;
- potentially high-volume transmission of usage data.

If this view is exposed over a reference point and implemented in a standard interoperable way, the choice of communications technology may emphasize the following non-exhaustive list of fitness-for-use criteria from 7.2:

- criteria based on interface-technology performance such as reliability, availability, survivability, response times, efficient protocol structure, large amounts of event data in real time, support for scoping and filtering capabilities;
- synchronization of data;
- scalability.

7.3.1.2 Characteristics of the EM view

The EM view may be described by the need for all of the following example characteristics:

- access to administrative functions of one or more NEs, such as NE installation functions, NE software installation/maintenance functions, NE assignable inventory, NE reserved resources management, aggregated usage data collection, NE security administration;
- access to functions that ascertain provisioning success in relationship to service level agreements (SLAs);
- access to functions that calculate NE-wide metrics such as NE performance, NE outages (SLA-related);
- access to functions that calculate certain NE metrics from an accumulation of NE data such as threshold crossing alert processing, performance trends analysis, alarm filtering and suppression (SLA-related);
- access to functions that control testing of circuits;
- access to raw data, less focus on real time, more focus on analysis of data.

If this view is to be exposed and implemented in a standard interoperable way, the choice of communications technology should emphasize the following non-exhaustive list of fitness-for-use criteria from 7.2:

- interface-technology criteria (e.g. filtering and scoping);
- user access;
- design of reusable components;
- information architecture details;
- scalability.

7.3.1.3 Characteristics of the NM view

The NM view may be described by the need for some of the following example characteristics:

- handle and analyse multiple network technologies to support the network level view;
- need to interface with IT environments and systems;
- interactions between customer care activities (and systems) and those functions within the NML systems that will oversee the management of the customer's services;
- interactions between NML systems handling activities such as alarm correlation, etc.;
- interactions between policy setting activities and those functions within the NML systems that must adhere to those policies;
- similar to a database interface requiring database management capabilities;
- work force management issues that are IT related and may require remote user access;
- flexibility to accommodate different network domains (e.g. ATM, SDH).

If this view is to be exposed and implemented in a standard interoperable way, the choice of communications technology should emphasize the following non-exhaustive list of fitness-for-use criteria from 7.2:

- portability;
- modularity;
- database design and other information architecture details;
- user access;
- security;
- ubiquity and ease of use.

7.3.1.4 Characteristics of the SM view

The SM view may be described by the need for some of the following example characteristics:

- more database like, requiring database management capabilities;
- IT-based with interfaces to all billing and order management applications;
- source of Quality of Service (QOS) details associated with connection establishment, connection quality, connection retention, billing integrity;
- possible concern over security issues related to the X interface.

If this view is to be exposed and implemented in a standard interoperable way, the choice of communications technology should emphasize the following non-exhaustive list of fitness-for-use criteria from 7.2:

- portability;
- modularity;
- database design and other information architecture details;
- security;
- ubiquity and ease of use.

7.3.1.5 Characteristics of the BM view

The BM view may be described by the need for some of the following example characteristics:

- ability to implement rule-based policy;
- IT-based environment;
- proprietary information content, variable data structures;

- high degree of security needed to protect access to proprietary information;
- requirement for database management capabilities;
- high degree of interconnection among interrelated systems to enable flow through;
- efficient sharing of data and processes among the connected applications;
- a variety of enabling technologies and standards for integration at the enterprise or domain levels, e.g. coexistence of IT and TMN standards;
- presence of business process functionality and independence from telecommunications functionality in some cases.

If this view is to be exposed and implemented in a standard interoperable way, the choice of communications technology should emphasize the following non-exhaustive list of fitness-for-use criteria from 7.2:

- database design and other information architecture details;
- portability.

7.3.2 Characteristics of inter-TMN reference points and interfaces

The x reference point exposed as an X interface allows the exchange of management information between TMNs found in different PTOs (different subsidiaries of the same telecommunications operator or different business partners). Additionally, the x reference point exposed as an X interface allows the exchange of management information between a customer and a service provider or network operator for the purpose of allowing the customer to perform some subset of management.

This management information exchange will most likely fall within the categories of service ordering, exchanging trouble report information, and billing. These management activities tend to be customer-service oriented versus network resource oriented, therefore x reference points exposed as X interfaces are usually realized between systems performing SML functionality.

Please refer to Recommendation M.3320 for X interface requirements.

7.4 Interface technology alternatives

The TMN comprises a number of accepted interface technologies. These mainly relate to open interfaces that allow the mixing and matching of equipment and software from many vendors to intercommunicate.

This is related mainly to exposed interfaces between different vendor's equipment either within the same TMN or between vendors in different TMNs. The evolving set of recommended technologies for achieving this is documented in Recommendations Q.811 and Q.812.

7.4.1 OSI systems management considerations

OSI systems management provides one of the TMN technology choices (see Recommendations X.700 and X.701). A summary of the key architectural concepts from a TMN perspective is presented below.

7.4.1.1 Object-oriented approach from OSI management

In order to allow effective definition of managed resources, the TMN methodology makes use of the OSI systems management principles and is based on an object-oriented paradigm. A brief presentation of the concept of objects is given below.

Management systems exchange information modelled in terms of managed objects. Managed objects 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. 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 modelling, i.e. to the interfaces over which communicating management systems interact and should not constrain the internal implementation of the telecommunications management system.

A managed object is defined by:

- the attributes visible at its boundary;
- the management operations that may be applied to it;
- the behaviour exhibited by it in response to management operations or in reaction to other types of stimuli. These can be either internal (e.g. threshold crossing) or external (e.g. interaction with other objects);
- the notifications emitted by it.

Additional considerations:

- there is not necessarily a one-to-one mapping between managed objects and real resources (which may be physical or logical);
- a resource may be represented by one or more objects. When multiple managed objects represent a resource, each object provides a different abstract view of the resource. Note that these objects might be coupled in their behaviour through physical or logical relationship;
- managed objects may exist that represent logical resources of the TMN rather than resources of the telecommunications network;
- if a resource is not represented by a managed object, it cannot be managed across the management interface. In other words it is not visible from the managing system;
- a managed object may provide an abstract view of resources that are represented by other managed objects;
- managed objects can be embedded, i.e. a managed object may represent larger resources that contain resources themselves modelled as sub-entities of the larger object.

The use of the methodology defined in Recommendation M.3020 has led to the identification of a generic network information model composed of a set of managed objects as defined in Recommendation M.3100. This model encompasses the whole of the TMN and is generally applicable to all networks. However, additional extensions to this will be required to allow for the details of differing managed network equipment types to be conveyed by the TMN.

7.4.1.2 Manager/agent concept

Management of a telecommunications environment is an information processing application. Because the environment being managed is distributed, network management is 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 (switching and transmission resources).

For a specific management association, the management processes will take on one of two possible roles. Note that the case where both roles can be taken during a single association requires further study. The description of the manager/agent concept given here is intended to reflect the definitions given in Recommendation X.701:

- manager role: the part of the distributed application that issues management operation directives and receives notifications;

- agent role: the part of the application process that manages the associated managed objects. The role of the agent will be to respond to directives issued by a manager. It will also reflect to the manager a view of these objects and emit notifications reflecting the behaviour 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.

7.4.1.3 Shared management knowledge (SMK)

Management functions (e.g. event management and state management) include an understanding of what options and which roles (e.g. manager or agent) are supported for each function. While trial and error is one method of gaining this understanding, the need for a more efficient mechanism is anticipated.

The actual instances of managed object classes that are available in a management interface form the most significant base of understanding needed by communicating management interfaces. CMIP scoping is a reasonable mechanism to provide most of this understanding. As with managed object classes, managed object instances may also be participating in relationships that need to be understood by a communicating management interface.

It is necessary to understand which managed object classes each management interface pairing supports. Since CMIP scoping is only capable of identifying instances of managed object classes, a more comprehensive mechanism is needed to understand the complete set of managed object classes supported, including those for which there is not presently an instance available. There may also be relationships (e.g. possible superior/subordinate-pairs for naming) between managed object classes. If so, a negotiation mechanism needs to support the development of this understanding as well.

Besides understanding which functions and managed objects are supported, the shared management knowledge (SMK) also includes an understanding of authorized management capabilities (e.g. permission to modify configurations, adjust tariffs, create or delete managed objects, etc.).

In order to allow effective definition of managed resources, the TMN methodology makes use of the OSI systems management principles and is based on an object-oriented paradigm. A brief presentation of the concept of objects is given below.

Management systems exchange information modelled in terms of managed objects. Managed objects 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.

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 modelling, i.e. to the interfaces over which communicating management systems interact and should not constrain the internal implementation of the telecommunications management system.

A managed object is defined by:

- the attributes visible at its boundary;
- the management operations that may be applied to it;
- the behaviour exhibited by it in response to management operations or in reaction to other types of stimuli. These can be either internal (e.g. threshold crossing) or external (e.g. interaction with other objects);
- the notifications emitted by it.

Additional considerations:

- there is not necessarily a one-to-one mapping between managed objects and real resources (which may be physical or logical);
- a resource may be represented by one or more objects. When multiple managed objects represent a resource, each object provides a different abstract view of the resource. Note that these objects might be coupled in their behaviour through physical or logical relationship;
- managed objects may exist that represent logical resources of the TMN rather than resources of the telecommunications network;
- if a resource is not represented by a managed object, it cannot be managed across the management interface. In other words it is not visible from the managing system;
- a managed object may provide an abstract view of resources that are represented by other managed objects;
- managed objects can be embedded, i.e. a managed object may represent larger resources that contain resources themselves modelled as sub-entities of the larger object.

The use of the methodology defined in Recommendation M.3020 has led to the identification of a generic network information model composed of a set of managed objects as defined in Recommendation M.3100. This model encompasses the whole of the TMN and is generally applicable to all networks. However, additional extensions to this will be required to allow for the details of differing managed network equipment types to be conveyed by the TMN.

7.4.2 Internet integration considerations

Telecommunications networks are evolving from digital circuit-switched technology to packet switched technologies with the emergence of the Internet. Leading packet-type technologies being deployed are ATM and the Internet Protocol (IP), with IP currently providing a common layer 3 infrastructure. This purveyance of packet technology as a universal transport gives impetus to voice over IP (VoIP) service with the result that today's telecommunications network will evolve from its present circuit-switched nature to a mixed packet/circuit-switched with an increasing proportion of IP traffic. In addition to VoIP, networks are evolving to carry other services over packet-switched networks that have traditionally been carried over circuit-switched networks, e.g. multimedia, video and facsimile. Many of the TMN concepts and methodologies developed for today's networks can be extended to encompass new or existing Internet-related concepts and technologies embodied in the Internet-related standards [e.g. simple network management protocol (SNMP)] for managing IP networks. Conversion from existing telecommunications network implementations to increasingly mixed circuit-switched and packet-switched based technologies will occur over time at varying rates from country to country. In this transition, the two technologies will coexist in different ratios in different countries. Therefore, the network management scenario should accommodate a flexible integrated management concept for network resources and operations.

Some points for examination include:

- Translation of SNMP Management Information Bases (MIBs).
- Scalability of SNMP managers.

7.4.3 CORBA integration considerations

Within general industry such as banking, manufacturing and financial the introduction and growth of Common Object Request Broker Architecture (CORBA) by corporate Information Technology (IT) departments as a solution to distributed computing is seen as being on the rise. This continued growth of CORBA has had the effect of reducing development costs and time-to-market for IT solutions. This is largely due to the increased availability of toolkits supporting standard Application Programming Interfaces (API) and wide spread knowledge within the IT community. This same effect – reduced costs and time-to-market for Operations Systems (OS) solutions in managing telecommunications Network Element (NE) equipment using CORBA has come under study within the telecommunication industry.

The existing universal standard in managing telecommunications is recognized as the Telecommunications Management Network (TMN). TMN allows for the use of CORBA at the X, or inter-TMN domain interface associated with the service management layer. However, more recently telecommunication standards experts have looked at including CORBA at the Q (OS to OS or OS to NE) interface. The prime factor for reviewing CORBA at the Q interface is to obtain the same advantages of cost savings, time-to-market and wide availability that exists in the larger IT industry, rather than for any deficiencies that exist in the current interface standard.

Currently the TMN standards at the Q interface, which is associated with information modelling and protocols, is the Guideline for Definition of Managed Objects (GDMO) and Common Management Information Protocol (CMIP). To introduce CORBA in this Q interface environment means that CORBA will have to adequately address the same telecommunications concerns and requirements that GDMO/CMIP did.

TMN standards efforts are under way in ITU-T to address this adoption of CORBA for application at the TMN Q interface.

Some points for examination include:

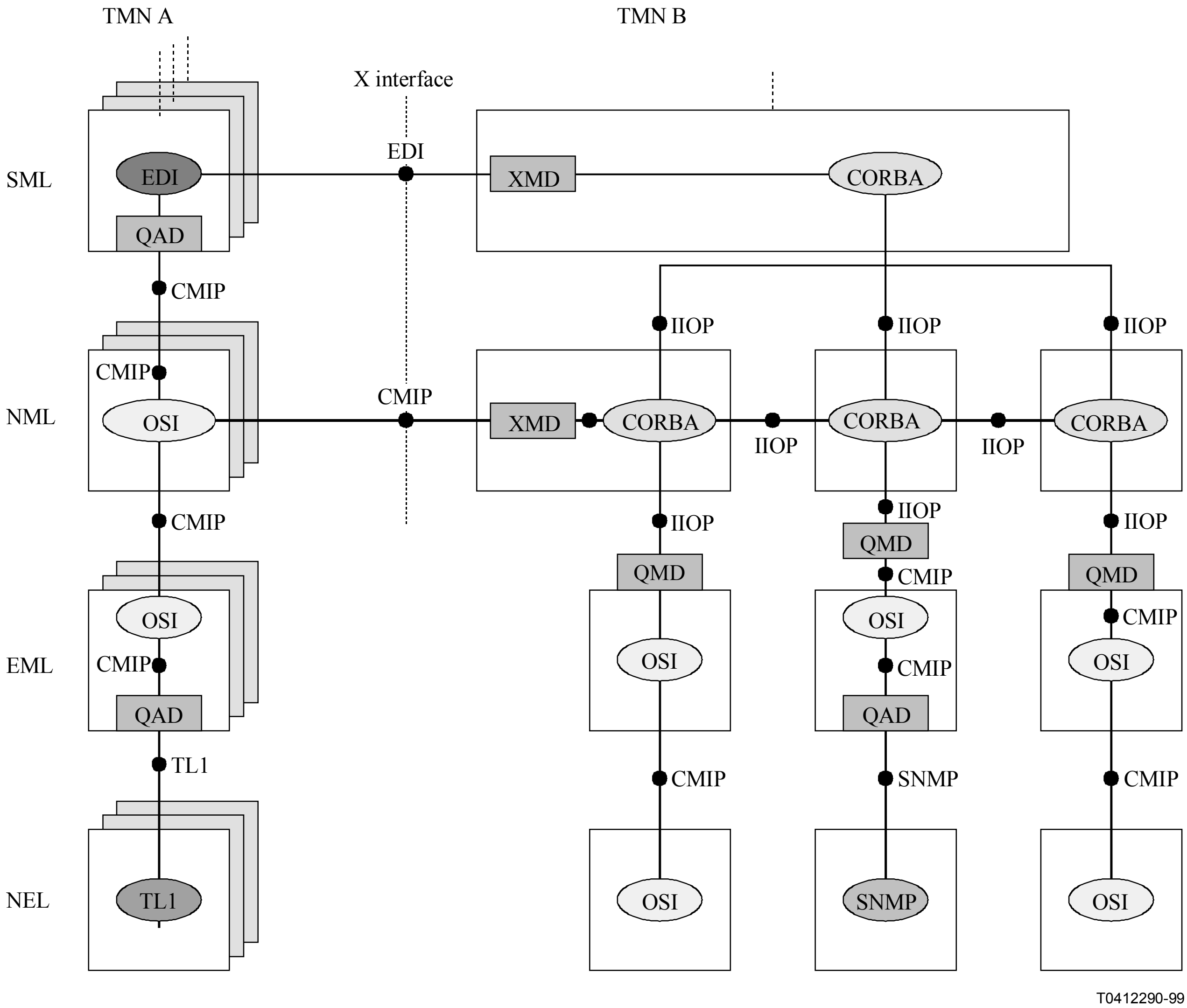
- use of existing models;
- scalability;
- support for multiple simultaneous managers;
- support of query capabilities;
- support of modification capabilities;
- support for selective access of attributes;
- support for multiple object query;
- support for multiple object set;
- autonomous notification with manager able to select the received notifications;
- definition of notification;
- containment relationship;
- support for deletion semantics;
- support for creation semantics.

7.4.4 Technology integration issues

Integration of new technology into a TMN can exert additional requirements on the TMN architecture and design. The following are some examples of considerations that need to be addressed:

- Where a new system has to interwork with an existing system, freedom to introduce new technologies has limitations. Systems in managed/managing roles have to share the exact same Management Information Bases (MIBs) in order to communicate. Consideration should be given to technologies that support interworking with existing systems. For example, with the CORBA environment services are being defined (e.g. notification services) to enable this management information base compatibility.
- Cost-effectiveness is strongly influenced by technology choice. Thus interface technology choice should be mindful of the impact on costs.

- TMN provides management services for many types of different management domains. Services, such as the CORBA naming and trading services, are one way to provide integration across these different domains.
- Different PTOs will operate in a manner streamlined to their own needs. It happens that no two PTOs will operate in the same way, as this is the manner in which commercial advantages are obtained over competitors.
- The use of mediation devices and adaptation devices (adaptors) are one way of integrating different technologies in a TMN. An example of TMN configurations accommodating different technologies within a TMN is shown in Figure 15. As additional interface technologies evolve and are introduced into TMN, Figure 15 shows possible configurations for interworking.



NOTE 1 – The ellipses in the figure represent part of a NEF in the network element layer (NEL) or OSF in the other layers (EML, NML and SML) with associated information representation to be used with the designated protocol over the interface.

NOTE 2 – XADs and QADs will change to XMDs and QMDs respectively as specific implementation technologies are approved for TMN applications.

Figure 15/M.3013 – Technology integration example

7.5 Directory and naming services

The architectural requirements described in Recommendation M.3010 cover some requirements to support distributed TMNs and TMN-interworking (or inter-domain management). The TMN architecture should:

- allow for geographic dispersion of a control over an aspect of the network operation;
- improve service assistance and interaction with a customer;
- provide a certain degree of reliability and security in the support of management functions;
- make it possible for a customer, value-added service provider and other PTOs to access management functions;
- make it possible to have different or the same management services at different locations, even if it accesses the same NE;
- make the interworking between separately managed networks possible, so that internetwork service can be provided between PTOs.

In general, directory services may be used to perform name to address resolution and capability assessment. Additionally, it may be used to support several security services, such as comparing a received authentication token to a value stored in the directory or the storage of public keys used in strong security mechanisms. Directory access and system functions have been added to allow access to the directory from each TMN function block. A directory defines a set of standardized operations, protocols, and security services that can be used by TMN domains. These directory features may be used to incorporate support for the following services:

- general information service for TMN-related information (yellow page services);
- global naming of managed objects;
- name/address resolution;
- representation of Shared Management Knowledge (SMK).

7.5.1 X.500 directory support

7.5.1.1 Users of a directory

TMN users (of a directory) may be classified into two groups of users: direct and indirect users. Direct users include TMN application entities and TMN system administrators. Indirect users include other types of users such as TMN subscribers or users of a customer management service.

NOTE 1 – Regardless of where a request for information (e.g. identity or capabilities) is initiated, the directory always returns the same set of values.

NOTE 2 – Access to the information stored in a directory may be denied because the requestor's credentials are insufficient per the access control permissions associated with the data stored in the directory.

7.5.1.2 Directory naming conventions

The directory employs a hierarchical naming convention that establishes as the start of the Directory Information Tree (DIT) the entity named root whose main value is empty (i.e. root = {}). Each Directory Object (DO) in the DIT has a globally unique name, called distinguished named. A Distinguished Name (DN) is a sequence of Relative Distinguished Names (RDNs), where each relative distinguished name represents a vertex in the DIT. A fully qualified DN is needed to name a leaf entry in the DIT. The directory also supports an alternative naming scheme, called *alias* or *alias-name*, which may be used to conceal the full topology of the DIT by using a relatively flat name space. The alias-name entry in the DIT contains the fully qualified distinguished name that the directory transparently uses to satisfy the requested directory operation. For example, a Network Element (NE) may have as its DN:

Fully qualified DN =

```
{country=us;organization=foobar;org_unit1=foobar1;org_unit1=foobar1;
 network=fantastic1;locality=my-town;NE_ID=1133441}
```

Alias name=`{network=fantastic1;net_el_ID="EMS1.1133441"}`

Where the syntax used is `<typename>=<string-value>` and `{}` identifies the start and end of the DN value.

To conceal the fully qualified distinguished name from the general public, the network provider may advertise the Alias-name to its trading partners, advising that access to information about network element 1133441 is accessed using the alias-name format.

NOTE 1 – Each TMN managed object is only associated to the root of the local MIT, this provides unique naming only in the context of the local MIT environment, i.e. the name is not globally unique.

NOTE 2 – Both TMN implementations and directory use the concept of distinguished name to uniquely name an object in it context. However, the directory would view a TMN distinguished name as a directory RDN.

7.5.1.3 Support for physical topology transparency

Within one TMN domain there may exist several closely related TMNs or TMN functional blocks of different management layers (network element, network, service, business layer). The directory may be used to provide transparency to the physical topology and geography of distributed TMNs in one or more TMN management domains.

7.5.1.4 Capability assessment of TMN elements

TMN entities may make use of the directory to assess the capabilities of a TMN component prior to attempting to communicate with it. The returned data may be used by TMN users to retrieve details about services, operators, networks, network elements, customer contracts, etc.

7.5.1.5 Managing non-TMNs network elements in a single TMN domain

The directory may be used to provide transparency to the physical communication vehicle needed to manage resources associated with a single TMN domain using non-TMN protocols. A TMN entity may use a directory to determine the communication address and protocols needed for communicating with that object.

7.5.1.6 NE reach information and capabilities of interest to TMN

The following non-exhaustive list illustrates the various types of information that may be supported by the directory:

- association information: The set of information related to association information may include:
  - the identity of the TMN element involved in the management subsystem;
  - the AE-titles and presentation address of the communication peer-entity;
  - the identity of management agents capable of providing the management functions based on the name of a managed object or optionally, the identity of a desired management capability;
  - the reachability information of a MO within a TMN domain whose address space and communication protocol is non-TMN compliant. For example, the kind of required credentials for communicating with the MO may be a candidate for the directory entry that represents or identifies a MO;
- management knowledge: The set of information related to management knowledge may include:
  - the application contexts supported by a named entity supporting TMN services;

– the management functional units supported by an application entity supporting TMN services;
– the management profile supported by an application entity supporting TMN services;
– the list of managed objects and classes associated with a management application entity;
– the identity of entities comprising TMN management domains;

- security support: The set of information related to security may include:
  – validating a presented password during association establishment;
  – determining access control information associated with information stored in a directory;
  – determining appropriate credentials employed during inter-TMN-domain communications;
- administrative usage: The set of information related to administrative usage may include:
  – a human administrator to manage access permissions associated with entries held in a directory;
  – using a directory in support of operating on the content of TMN data store and sub-tree structure and to verify the access permissions associated with the requestor and the target object;
  – the contact information (e.g. e-mail addresses) and roles of persons involved in TMN management.

7.5.1.7 Integration of directory and TMN information architectures

Figure 16 depicts the relationships between the Directory Objects (DOs) represented in a Directory Information Base (DIB) (and named in the DIT) and the Managed Objects (MO) represented in a Management Information Base (MIB) (and named in a MIT). As explained in 7.5.1.2, each DO named in the DIT is associated with a single globally unique *root,* thereby providing a means for binding globally unambiguous names to DO in an open environment.

If Managed Objects (MOs) need to be made visible in a global name space, e.g. for inter-domain management or TMN interworking, a globally unique name may be required for these MOs. As illustrated in Figure 16, this can be achieved by associating the *name(s)* used to name object a local MIB to DOs named in the global DIT, i.e. have the DO point to MOs in a local MIB. A naming relationship among DOs and the MIT's root MO (i.e. the system MO class defined in Recommendation X.721 or network MO class defined in Recommendation M.3100) has been defined in Recommendations X.701 and X.750.

NOTE 1 – MIT and DIT are similar in nature in that each characterizes a hierarchical naming convention used the context of each service type. Likewise, MIB and DIB are similar in that they characterize an object oriented information base known to each service type. Both service types employ the use of a schema to identify relationships about the managed objects.

NOTE 2 – The root object in TMN is domain specific, whereas the root object in the directory is the same across directory domains. Consequently, the directory naming convention enables the same results to be returned regardless where a query request is originated, whereas the results of a TMN query return results relevant to domain where the managed object resides.

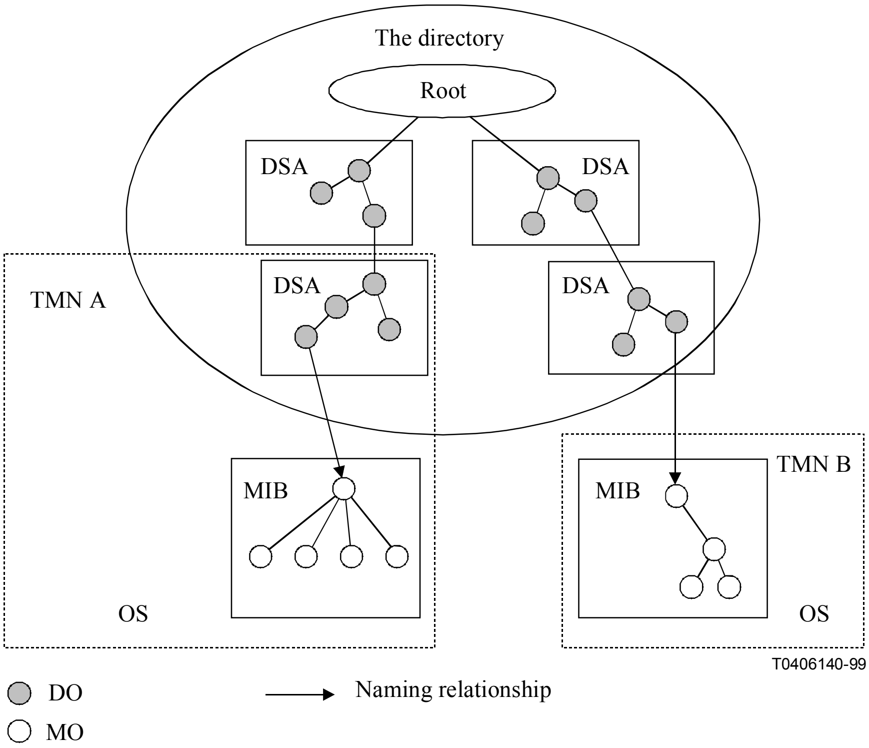


Figure 16/M.3013 – Integrated directory and TMN information architecture

DOs may be represented by general information types defined in Recommendation X.520: selected attribute types, Recommendation X.521: selected object classes. The set of directory information types may be extended to support specific application needs (such as NE descriptive or capability information) by applying application specific directory schema extensions specified in the X.700-series Recommendations (e.g. Recommendation X.750 management knowledge management function), in M.3000-series and other Recommendations (e.g. in the X.400-series). Some of the information types defined in Recommendations X.520, X.521 may be useful in representing TMN-related MOs.

7.5.1.8 Implementation considerations

MO information may be represented or warehoused held the directory's DIB where access to this information is made globally available, although access to specific DOs may be limited to authorized TMN management functions or persons. Furthermore, the information held in the DIB may be as detailed (or simple) as dictated by business needs.

Remote access to a directory DSA, which is modelled as the manager of the DOs under its control, is through the use of a Directory User Agent (DUA). Communication between a DUA and DSA is achieved by using the Directory Access Protocol (DAP) or the lightweight DAP (L-DUA) specified in the IETF RFC 1777. The DUA/L-DUA uses DAP/LDAP (respectively) to convey a set of abstract operations, which operates on information known to the DSA or federation of cooperating DSAs.

The directory may be implemented as a collection of distributed and cooperating DSAs, or a single centralized DSA. In a distributed directory, DSAs use the Directory System Protocol (DSP) to relay requests received from a DUA or another DSA to another who is believed to have access to the requested DOs or attributes associated with a directory entry or by returning a *referral* to the requesting DUAs. Implementers may choose the design most appropriate to their environment.

A TMN application entity (TMN-AE) wishing to retrieve information held in the directory may implement the DUA functionality co-resident with the TMN-AE. In this case, a TMN-AE appears to the directory as a DUA, which originates DAP (or LDAP) requests.

NOTE 1 – Colocated TMN-AE and a lightweight DUA modules, which originate LDAP formatted directory retrieval or comparison requests, is the most common configuration today. Full DUA functionality is not normally needed by TMN-AEs or TMN users.

However, the TMN-AE may choose to appear to the directory as a DSA, in which case it supports the chaining or broadcasting of directory requests to other DSAs. When the implementation chooses to behave externally as a DSA, it supports the DSP protocol across a bidirectional interface. Figure 17 illustrates these two cases. In both instances, the local interface between the TMN-AE and directory entity is outside of the scope of this Recommendation.

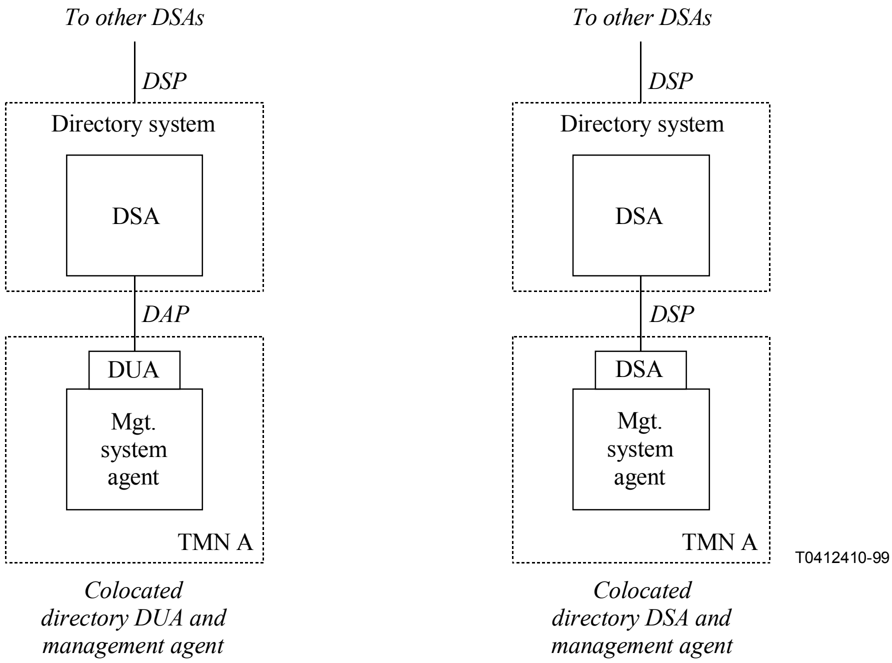


Figure 17/M.3013 – Illustration of likely configurations enabling TMN use of directory

NOTE 2 – A consequence of implementing a DAP interface is that the implementation knows of one or more DSAs that may hold the desired information where each DSA is external to the TMN environment. In the directory, this concept is known as "referral".

NOTE 3 – If an implementation chooses to expose only a DSP interface, then the implementation need only support DUA services, and not DAP for LDAP.

NOTE 4 – The IETF environment promotes the use of LDAP (IETF RFC 1777), "The lightweight directory access protocol" as its DUA client implementation. Currently, it is widely available and supports a simplified DAP directly onto TCP/IP for transmission over a TCP/IP stack, instead of the historical protocol OSI stack.

7.5.2 OSI naming and addressing

For the successful introduction of a TMN [within an Open Systems Interconnection Environment (OSIE)] into an PTO, a logical, integrated naming and addressing scheme for identifying and locating the various communications objects within a TMN is critical. In order to locate TMN systems and identify various entities within each system, unambiguous naming methods are required.

The following text provides information on the issues involved in creating and using naming and addressing schemes for use within the TMN environment.

7.5.2.1 Principles for naming schemes

This subclause presents some principles for the design of naming schemes. Some properties of the names are:

- they are required to be unique or unambiguous;
- they are primarily for use by automated equipment;
- mappings between various names such as, from Application Entity (AE) title to presentation address, are expected to involve "directory" functions;
- the directories may be held locally or off-system.

7.5.2.2 Unambiguous naming

When names are required to be unique or unambiguous (globally), a mechanism is required for coordinating naming activities among PTO. This is generally achieved at the global level by systematically dividing the set of all possible names into subsets.

The relevant OSI names and addresses that should be unambiguous on a wide scale are:

- Network Service Access Points (NSAP) addresses;
- system titles [including applications process titles and Application Entity (AE) titles].

The relevant OSI names and addresses that should be unambiguous with a particular system are:

- selectors;
- AE-qualifiers.

7.5.2.3 Addresses

An AE-title maps to a presentation address that may be represented by the *tuple*:

- (P-selector, S-selector, T-selector, list of network addresses.)

The selectors are identifiers that are local to a system, that is, they can be set independently with regard to other systems. However, a set of standardized values for selectors should be established for administrative reasons. It is recommended that there should be as few assigned selector values as possible. Furthermore, the lengths should be short.

The NSAP should be based on Recommendation X.213.

7.5.3 CORBA naming and addressing

CORBA is based on a distributed object model. The objects encapsulate both data and operations. CORBA provides an underlying architecture for the objects to communicate with each other, and for object to be distributed. CORBA provides services to help ease application development. To permit objects using different Object Request Brokers (ORBs) to communicate with each object is identified by an Interoperable Object Reference (IOR). The IOR contains information about the interface type, what protocol(s) are supported, and specific information associated with each protocol (e.g. TCP/IP support included host name, port number, and an object key). This information is opaque (hidden) to the application, but it is necessary for the ORBs so that a client can communicate with a selected object. IORs can be passed as a parameter in interface operations. This provides sophisticated capabilities to create dynamically interfaces using the factory design pattern.

7.5.3.1 CORBA naming service

The CORBA naming service is similar to a telephone directory. It is possible to look up number (address) when given a known name (e.g. a mapping is provided from a person's name to a telephone number). The CORBA naming service provides a similar function for mapping a name to an object reference.

It is also possible for an object to be identified by several names, i.e. an object may have several aliases. The naming service supports hierarchies of name to object references formed with naming contexts. The relationships between names and contexts can be depicted in a naming graph. The naming service provides very few restrictions on how to create naming graphs. While there are always situations that break a general guide, it is not advised to use loops in the naming graph, as this can lead to an infinite number of paths. This is understood to complicate naming administration and is not recommended. In some circumstances this may be needed, e.g. if the naming service is used as a front end to an existing naming service that already support looped contexts. Where names cross several machines in different geographic locations, the naming service can be federated. The actual details of this are hidden from the application program that provides interoperable name to location resolution.

7.5.3.2 CORBA Interoperable Naming Service (INS)

This is a service extension to the naming service that permits initial access to a naming service from other systems in a multi-vendor manner. The mode of operation is similar to techniques found on the Web using URLs and search engines.

7.5.3.3 CORBA trader service

The CORBA trader is a service that permits a client to browse what services are available, without *a priori* knowledge of what services exist. The trader service equates to the telephone directory yellow pages. Each entry in the trader service is an advertisement for a capability. This allows a client to query the trader to locate implementations that can satisfy the clients requirements.

Traders could be utilized for bandwidth and QOS/COST negotiation in an automated manner. The client can make queries to the trader, which define options and values that are acceptable to the client. The trader may return a number of service offers that satisfy the client's request. The client may then select one of these offers to provide the desired service.

APPENDIX I

TMN architecture considerations for selected telecommunications managed areas

The TMN functional, information and physical architectures must keep pace with the introduction of new technologies, services and evolving network infrastructures. New technologies such as ATM (asynchronous transfer mode), new services such as UPT (universal personal telecommunication) and evolving network infrastructure such as IN [intelligent network(s)] must be accommodated within the TMN. For example, the TMN must be able to test, deploy and support rapid service creation in IN.

This appendix addresses how TMN is expected to manage the IN and its associated services and SDH transport network applications.

I.1 Intelligent Networks (INs)

The TMN provides capabilities to manage telecommunications infrastructures including services, networks and network elements.

The goals of IN management are to:

- provide effective management of the network infrastructure required to support IN based services;
- provide/support effective management of the IN service creation environment;
- ensure rapid and efficient service deployment;
- provide for the efficient management of IN-based services.

The management of the IN infrastructure and service creation environment are not dealt with in the body of this appendix. The management of the IN infrastructure (network elements, signalling protocols, etc.) is considered to be performed as for other, non-IN, infrastructures (e.g. SDH, ISDN). The management of the service creation environment and its relation with the TMN are for further study.

The advantages of using the TMN for the management of IN are:

- a common management philosophy for the management of INs and other networks (e.g. SDH, ISDN) services and equipment;
- economies through the use of common techniques. These economies can arise from the reuse of software developed for one application in another;
- unification of management processes and the use of common management systems (e.g. common fault, accounting, performance and security systems).

I.1.1 IN activities within the scope of TMN management

The TMN can be involved with all of the steps identified below.

The TMN manages the communication of management information between the service creation environment and the telecommunications networks and management resources. The actual split between "off line" service creation and interaction with the TMN or the network via the TMN is for further study.

I.1.1.1 Service creation

The creation of (new) services consists of several steps, which are summarized, in the service creation process. The different steps are:

- service specification;
- service development;
- service verification;
- service creation deployment;
- service creation management.

There is partitioning of functionality between the TMN and the service creation environment.

I.1.1.2 Service deployment

Service deployment deals with the installation of software and data (e.g. created by the SCEF), into the management systems associated with the service and the network on which the service is being deployed (e.g. the SCF/SDF).

Service deployment functions allocate information to the relevant parts of the network and manage that information. This information includes:

- service scripts;
- service generic data;
- signalling routing data;
- trigger data;
- specialized resource data;
- service testing;
- service provisioning.

Service provisioning collects service specific data and controls the installation and administration of this data in subscriber databases and contact databases.

I.1.1.3 Service operation control

Service operation control performs service maintenance and updates information (e.g. service generic, customer specific data, signalling routing, trigger data and specialized resource data) and security.

I.1.1.4 Billing

Billing functions include the management of the generation, collection and storage of call records and the introduction and modification of tariffs.

I.1.1.5 Service monitoring

Service monitoring includes the measurement, analysis and reporting of service usage and performance.

I.1.2 IN concepts

A key concept in IN is the IN conceptual model that comprises four planes:

- the SERVICE PLANE (SP) represents an exclusively service oriented view (no implementation knowledge);
- the GLOBAL FUNCTIONAL PLANE (GFP) models network functionality from a network wide view. As such the IN structured network is viewed as a single entity;
- the DISTRIBUTED FUNCTIONAL PLANE (DFP) models a distributed view of an IN structured network;
- the PHYSICAL PLANE (PP) models the physical aspects of IN structured networks;
- in addition, there are general aspects defined for the intelligent network application protocol (INAP).

I.1.3 Relationship between TMN and IN concepts

Both TMN and IN make physical/implementation specific aspects independent of the logical/functional aspects.

Although the TMN has similar concepts as those contained in the service plane and global functional plane (the TMN has management services and function sets), these concepts do not map directly into a TMN architecture.

However, the distributed functional plane and physical plane of the IN can be mapped into the TMN logical and physical architectures.

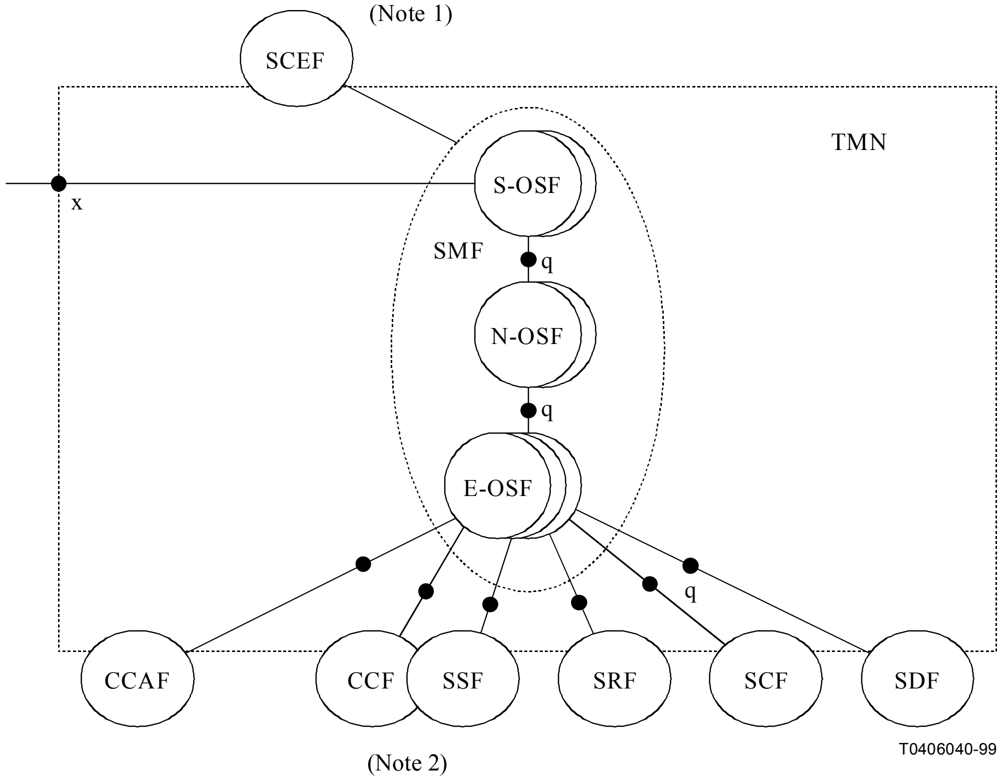
Table I.1/M.3013 – Correspondence between IN and TMN concepts

	IN	Relationship	TMN
Service plane	IN service	Corresponding level of abstraction	TMN management service
	IN service feature	Corresponding level of abstraction	TMN function set
Global functional plane	SIB	Corresponding level of abstraction	To be determined
Distributed functional plane	Functional entity	Allocated to	Function block
	Functional entity action	Corresponding level of abstraction	Management Application Functions (MAF)
	Information flow element	Corresponding level of abstraction	Managed object(s)
	Information flow element	Corresponding level of abstraction	Attribute/operation/notification
	Reference point	Equivalent to	Reference point
Physical plane	Physical entity	Corresponding level of abstraction	Resource
	Interface	Corresponding level of abstraction	Interface

Table I.1 relates the IN and TMN concepts. Please note that the relationships only indicate an approximate correspondence. It should be noted that the IN planes and the TMN layers represent different concepts, it is not appropriate to try to show a direct relationship between them.

I.1.4 Mapping of IN distributed functional plane to the TMN logical architecture

Figure I.1 shows how the FEs in the IN distributed functional plane can be considered as TMN function blocks. CCAF, SSF, SCF, SDF, CCF and SRF are TMN network element functions and SMF is equivalent to one or more TMN OSFs.



CCAF	Call Control Access Function
CCF	Call Control Function
E-OSF	Element management layer – Operations Systems Function
N-OSF	Network management layer – Operations Systems Function
SCF	Service Control Function
SCEF	Service Creation Environment Function
SDF	Service Data Function
S-OSF	Service management layer – Operations Systems Function
SRF	Specialized Resource Function
SSF	Service Switching Function

NOTE 1 – SCEF location and reference points to OSFs are for further study.

NOTE 2 – The SSF and CCF functionality are assumed collocated in IN.

Figure I.1/M.3013 – A possible mapping of the IN service processing functional entities onto a TMN functional architecture

I.1.5 Mapping of IN physical plane to the TMN physical architecture

When IN functionality is realized in physical systems, the reference point between functionality in one system and functionality in another system becomes an interface.

In the case of management interfaces, these can be translated into TMN interfaces.

Figure I.2 illustrates the relationship between IN physical entities to the TMN managed objects and physical architecture.

Figure I.3 illustrates the mapping of IN physical entities to the TMN physical architecture.

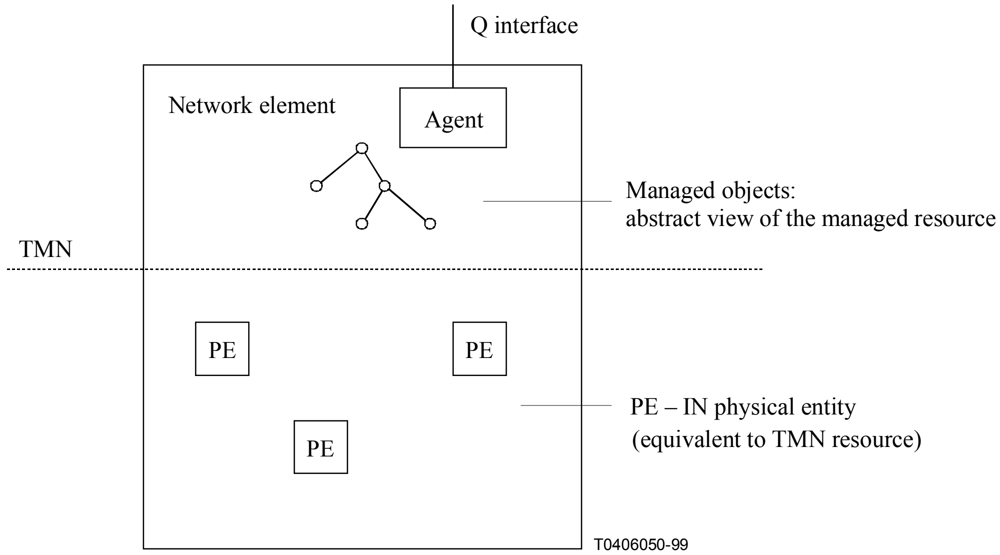
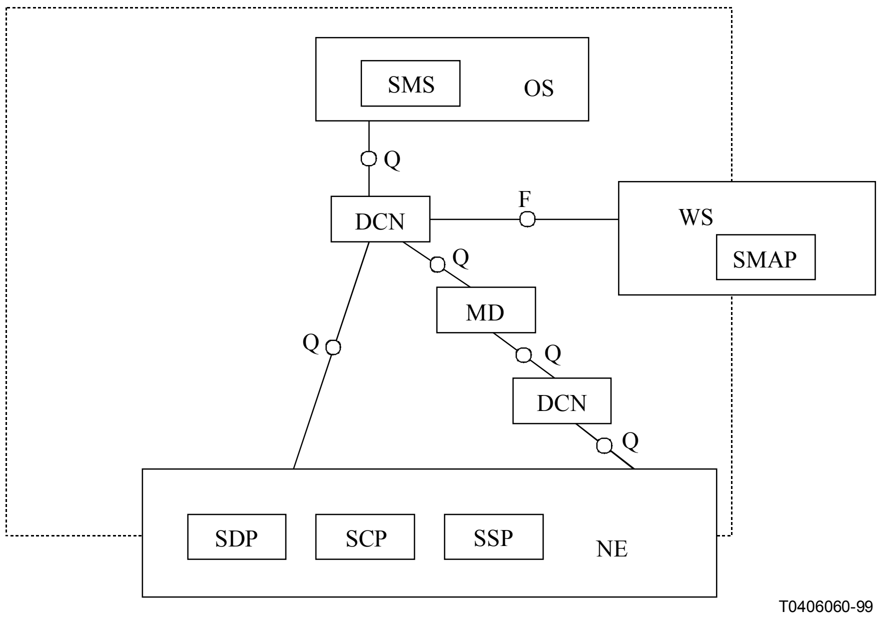


Figure I.2/M.3013 – Relationship of IN physical entities to the TMN



DCN Data Communication Network
MD Mediation Device
SCP Service Control Point
SDP Service Data Point
SMAP Service Management Access Point
SMS Service Management System
SSP Service Switching Point

Figure I.3/M.3013 – Mapping of IN physical entities to the TMN physical architecture

Table I.2 provides a possible mapping of the IN physical and functional entities onto the TMN physical and functional architectures.

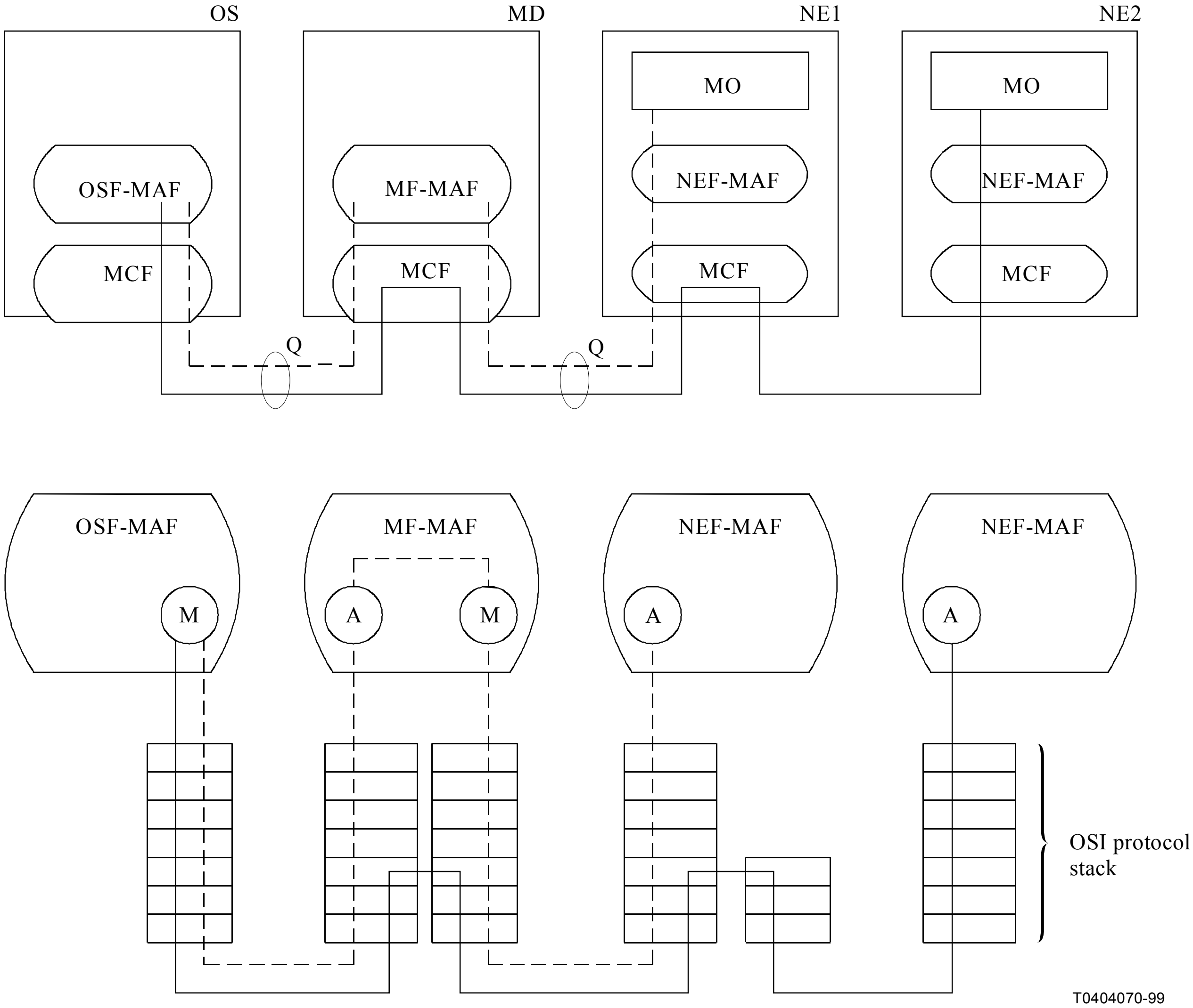
Table I.2/M.3013 – A possible mapping for the IN physical entities onto the TMN function and building blocks

IN Physical Entity (PE)	IN Functional Entity (FE)	TMN function blocks	TMN building blocks
SDP (service data point)	SDF (service data function)	NEF	NE
SCP (service control point)	SCF (service control function)	NEF	NE
SSP (service switching point)	CCAF (call control access function) CCF (call control function) SSF (service switching function) SRF (specialized resource function)	NEF	NE
SMS (service management system)	SMF (service management function) SMAF (service management access function SCEF (service creation environment function)	E-OSF, N-OSF, S-OSF WSF (Note)	OS WS (Note)
SMAP (service management access point)	SMAF (service management access function)	WSF	WS
SCEP (service creation environment point)	SCEF (service creation environment function	(Note)	(Note)
NOTE – The relationship between SCEF and TMN function blocks is for further study.			

I.2 Transport network

I.2.1 SDH communications examples

Figures I.4 and I.5 are examples from the SDH environment showing how some devices may provide a routing and relaying function (via MCF) while in other cases they intervene at information model level, e.g. by providing information conversion or even additional functions. In a cascaded arrangement some devices may, therefore, only serve as communication relays, while some others will include mediation functions.



- - - - } Information paths

A	Agent
M	Manager
MCF	Message Communication Function
MF	Mediation Function (transformation function)
MF-MAF	MF – Management Application Function
MO	Managed Object
NE	Network Element
NEF	Network Element Function
NEF-MAF	NEF – Management Application Function
OSF	Operations Systems Function
OSF-MAF	OSF – Management Application Function

Figure I.4/M.3013 – SDH functional configuration examples

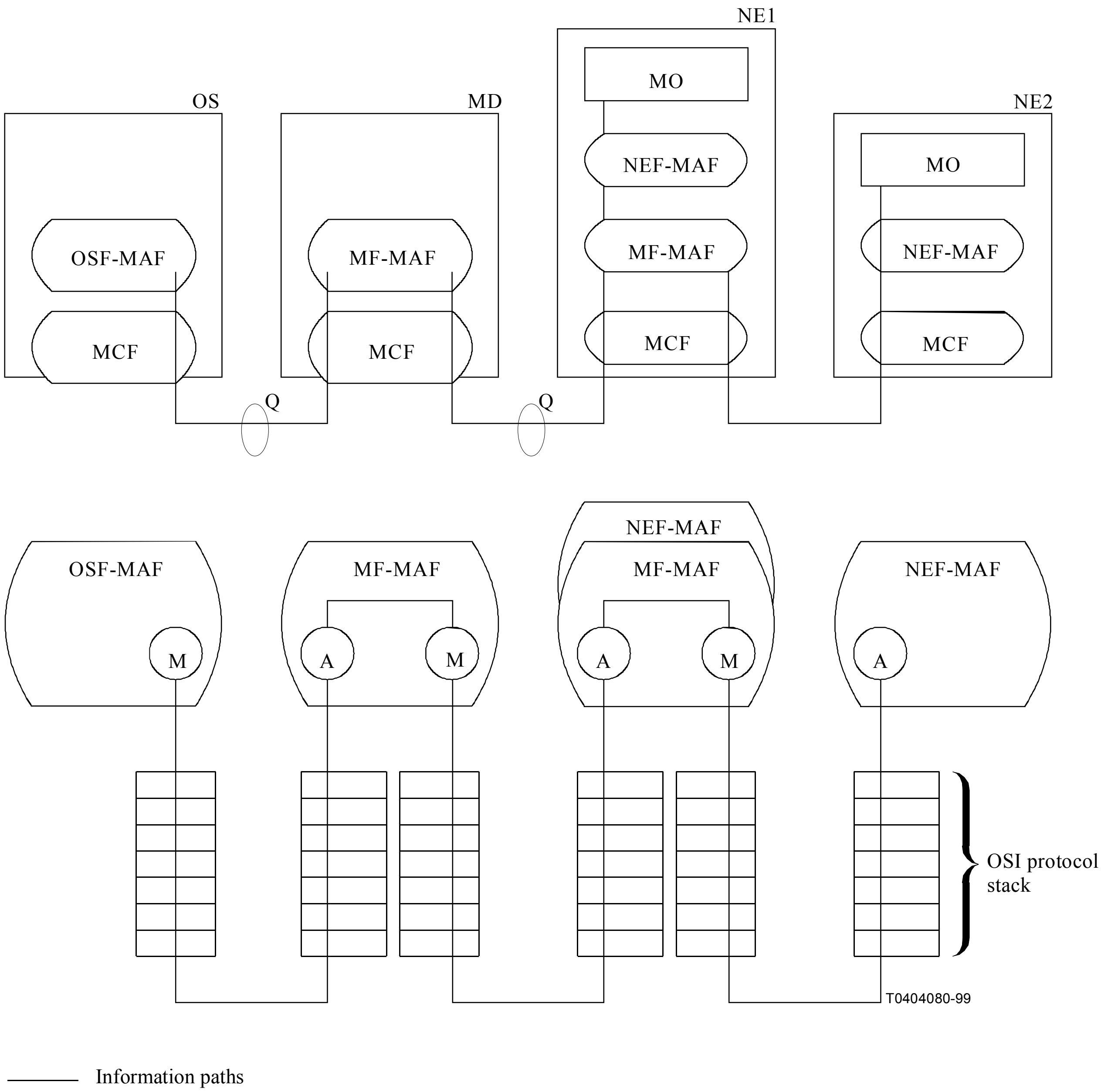


Figure I.5/M.3013 – SDH functional configuration examples

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

18260

Printed in Switzerland
Geneva, 2000