Recommendation

ITU-T G.7718/Y.1709 (2020) Amd. 1 (11/2022)

SERIES G: Transmission systems and media, digital systems and networks

Data over Transport – Generic aspects – Transport network control aspects

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Internet protocol aspects – Operation, administration and maintenance

---

Framework for the management of management-control components and functions

Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
General	G.7000–G.7099
Transport network control aspects	**G.7700–G.7799**
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

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

Recommendation ITU-T G.7718/Y.1709

Framework for the management of management-control components and functions

Amendment 1

Summary

Recommendation ITU-T G.7718 contains the framework for ASON management. It places automatically switched optical network (ASON) management within the TMN context and specifies how the TMN principles may be applied. A management view of the ASON control plane is developed. This view provides the bases for the ASON management requirements specified in this Recommendation. Identifier spaces needed in ASON management are specified. Examples of management system structures and ASON related management applications are contained in the appendices.

The 2010 version of this Recommendation adds the requirements to support permanent connection to soft permanent connection migration, configuration of routing controller adjacencies, call detail record for accounting management, and refresh of management plane and control plane views.

The 2020 edition of the Recommendation extends the scope from ASON management to the aspects of management of MC (management and control) components and functions.

Amendment 1 to Recommendation ITU-T G.7718 (2020) updates management requirements to align with the recent changes to Recommendation ITU-T G.7701, ITU-T G.7702 and ITU-T G.7703.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.7718/Y.1709	2005-02-13	15	11.1002/1000/1892
2.0	ITU-T G.7718/Y.1709	2010-07-29	15	11.1002/1000/10897
3.0	ITU-T G.7718/Y.1709	2020-10-29	15	11.1002/1000/14542
3.1	ITU-T G.7718/Y.1709 (2020) Amd. 1	2022-11-13	15	11.1002/1000/15146

Keywords

Context management, management-control system, management requirements, MC components, MC functions, MCS.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. 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, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.7718/Y.1709

Framework for the management of management-control components and functions

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.7718/Y.1709 (2020).

1 Scope

This Recommendation addresses the management aspects of the components that provide the functions of managing and/or controlling the transport network resources. The concept whereby management and control functions are considered to be a continuum is known as the management-control continuum (MCC); i.e., it expresses the view that management and control functions are essentially the same and, thus, they can be grouped into one set of functions. This set of functions is collectively called management and control (MC) functions. A component that provides one or more MC functions is called an MC component.

1.1 MC functions

The control functions considered for management in this Recommendation include the common control functions specified in [ITU-T G.7701], the SDN architecture specific control functions defined in [ITU-T G.7702] and the ASON architecture specific control functions defined in [ITU-T G.~~8080~~7703].

The management functions within the scope of ITU-T G.7718 in general follows the TMN principles specified in [ITU-T M.3010] and include the generic fault management, configuration management, account management, performance management and security management (FCAPS) functions specified in [ITU-T X.700], the transport-technology-neutral FCAPS management functions in [ITU-T G.7710], and the transport-technology-specific FCAPS management functions in [ITU-T G.784 series] for SDH, [ITU-T G.874 series] for OTN, [ITU-T G.8051 series] for Ethernet, [ITU-T G.8152 series] for MPLS-TP, [ITU-T G.7721 series] for synchronization, etc.

1.2 MC components

MC components provide functions for managing and controlling transport resources. They are used to construct scenarios for explaining the operation, interface and architecture of MCS. The related management operations/interfaces are studied in the aspects listed below:

– Between MC components;
– Between MC component and transport resources;
– Between administrative role (e.g., management-control system (MCS)) and MC components;
– MC components for control purposes are defined in [ITU-T G.7701], [ITU-T G.7702] and [ITU-T G.~~8080~~7703], including:
  – Connection controller (CC)
  – Calling/called party call controller (CCC)
  – Discovery agent (DA)
  – Directory service (DS)
  – Link resource manager (LRM)

  - Network call controller (NCC)
  - Protocol controller (PC)
  - Routing controller (RC)
  - Resource notification component (RNC)
  - Termination and adaptation performer (TAP)
- MC components for management purposes are defined in [ITU-T G.7710]. For example, Figure 7 of [ITU-T G.7710] depicts the fault management related components within the equipment management function (EMF) and their functional interactions. Illustration of the operations/interfaces to and from each of the fault management functions/components are described in clauses 7.2.1 to 7.2.14 of [ITU-T G.7710]. MC components for configuration management and performance management are specified in clauses 8 and 10.2 of [ITU-T G.7710].

1.3 Managing the MC functions and components

This Recommendation addresses the management, including administration, of the MC components and functions that manage and/or control the transport network resources.

In this edition of the Recommendation, only the control components and functions (i.e., those defined in [ITU-T G.7701], [ITU-T G.7702], and [ITU-T G.~~8080~~7703]) are considered. Management of the management components and functions (i.e., those defined in [ITU-T G.7710] and the transport-technology-specific Recommendations [ITU-T G.874], [ITU-T G.8051], etc.) are for study in future editions of this Recommendation.

The management aspects covered in this Recommendation include the management requirements of the MC components and the interfaces from the MC components to the administrative context and the client contexts. The management requirements include, but are not limited to, lifecycle management of the components and the contexts for transport services and/or resource, ranging from simple static connectivity service to client specific virtual network service.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.784] Recommendation ITU-T G.784 (2008), *Management aspects of synchronous digital hierarchy (SDH) transport network elements*.

[ITU-T G.798] Recommendation ITU-T G.798 (2017), *Characteristics of optical transport network hierarchy equipment functional blocks*.

[ITU-T G.800] Recommendation ITU-T G.800 (2016), *Unified functional architecture of transport networks*.

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.806] Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.874] Recommendation ITU-T G.874 (2017), *Management aspects of optical transport network elements*.

[ITU-T G.875] Recommendation ITU-T G.875 (2020~~17~~), *Optical transport network: Protocol-neutral management information model for the network element view*.

[ITU-T G.7701] Recommendation ITU-T G.7701 (2022~~16~~), *Common control aspects.*

[ITU-T G.7702] Recommendation ITU-T G.7702 (2022~~18~~), *Architecture for SDN control of transport networks.*

[ITU-T G.7703] Recommendation ITU-T G.7703 (2021), *Architecture for the automatically switched optical network*.

[ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020~~12~~), *Common equipment management function requirements*.

[ITU-T G.7711] Recommendation ITU-T G.7711/Y.1702 (2022~~18~~), *Generic protocol-neutral management Information Model for Transport Resources*.

[ITU-T G.7712] Recommendation ITU-T G.7712/Y.1703 (2019~~10~~), *Architecture and specification of data communication network*.

[ITU-T G.7713] Recommendation ITU-T G.7713/Y.1704 (2009), *Distributed call and connection management (DCM)*.

[ITU-T G.7713.1] Recommendation ITU-T G.7713.1/Y.1704.1 (2003), *Distributed call and connection management (DCM) based on PNNI*.

[ITU-T G.7713.2] Recommendation ITU-T G.7713.2/Y.1704.2 (2003), *Distributed call and connection management: Signalling mechanism using GMPLS RSVP-TE*.

[ITU-T G.7713.3] Recommendation ITU-T G.7713.3/Y.1704.3 (2003), *Distributed call and connection management: Signalling mechanism using GMPLS CR-LDP*.

[ITU-T G.7715] Recommendation ITU-T G.7715/Y.1706 (2002), *Architecture and requirements for routing in the automatically switched optical networks*, including Amendment 1 (2007).

[ITU-T G.7715.1] Recommendation ITU-T G.7715.1/Y.1706.1 (2004), *ASON routing architecture and requirements for link state protocols*.

[ITU-T G.8051] Recommendation ITU-T G.8051/Y.1345 (2020), *Management aspects of the Ethernet transport (ET) capable network element*.

~~[ITU-T G.8080] Recommendation ITU-T G.8080/Y.1304 (2012), *Architecture for the automatically switched optical network (ASON).*~~

[ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*, plus Amendment 1 (2003), and Amendment 2 (2005).

[ITU-T M.3100] Recommendation ITU-T M.3100 (2005), *Generic network information model*.

[ITU-T M.3120] Recommendation ITU-T M.3120 (2001), *CORBA generic network and network element level information model*, plus Amendment 1 (2002), and Amendment 2 (2003).

[ITU-T X.700] Recommendation ITU-T X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications*.

[ITU-T X.731] Recommendation ITU-T X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems management: State management function*.

3 Definitions

No new terms and definitions are defined in this Recommendation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AP Access Point

ASON Automatically Switched Optical Network

CC Connection Controller

CCC Calling/called party Call Controller

CCN Control Communication Network

CoS Class of Service

CP Connection Point

CPI Control Plane Interface

CRUD Create/Read/Update/Delete

CTP Connection Termination Point

DA Discovery Agent

DCN Data Communications Network

DS Discovery Service

ECC Embedded Communication Channel

EMF Equipment Management Function

EMS Element Management System

E-NNI External Network-Network-Interface

FC Forwarding Construct

FCAPS Fault management, Configuration management, Account management, Performance management and Security management

FD Forwarding Domain

FEF Fault Event Filtering

FEPt Forwarding End Port

FP Forwarding Point

GNE Gateway Network Element

GoS Grade of Service

I-NNI Internal Network-Network-Interface

LCAS Link Capacity Adjustment Scheme

LRM Link Resource Manager

LT Layer Termination

LTP Logical Termination Point

MC Management-Control

MCC	Management-Control Continuum
MCS	Management and Control System
NCC	Network Call Controller
NE	Network Element
NMS	Network Management System
OAM	Operation, Administration and Maintenance
OSS	Operations Support System
OTN	Optical Transport Network
PC	Protocol Controller
PTP	Physical Termination Point
RA	Routing Area
RC	Routing Controller
RNC	Resource Notification Component
SC	Switched Connection
SDN	Software-Defined Networking
SNP	Subnetwork Point
SNPP	Subnetwork Point Pool
SPC	Soft Permanent Connection
SRG	Shared Risk Group
TAP	Termination and Adaptation Performer
TMN	Telecommunications Management Network
TP	Traffic Policing
TPE	Termination Point Encapsulation
TTP	Trail Termination Point
UNI	User-Network-Interface
UNI-C	User-Network Interface – Client
UNI-N	User-Network-Interface – Network
VCAT	Virtual Concatenation
VN	Virtual Network

5 Conventions

In this Recommendation, the following requirement key words are used:

– SHALL: This word means that the definition is an absolute requirement.

– SHALL NOT: This phrase means that the definition is an absolute prohibition.

– SHOULD: This word means that there may exist valid reasons in particular circumstances to ignore the requirement.

– MAY: This word means that the requirement is truly optional.

6 Architecture of managing MC components and functions

This clause briefly introduces the concept of management and control continuum, the management and control system, their relationship to the MC components, transport resource and service, and management aspects of MC component and functions.

6.1 MCC concept

As defined in [ITU-T G.7701], management and control functions are considered to be a continuum and the concept of management-control continuum expresses the view that management and control functions are essentially the same and, thus, management and control functions can be grouped into one set of MC functions.

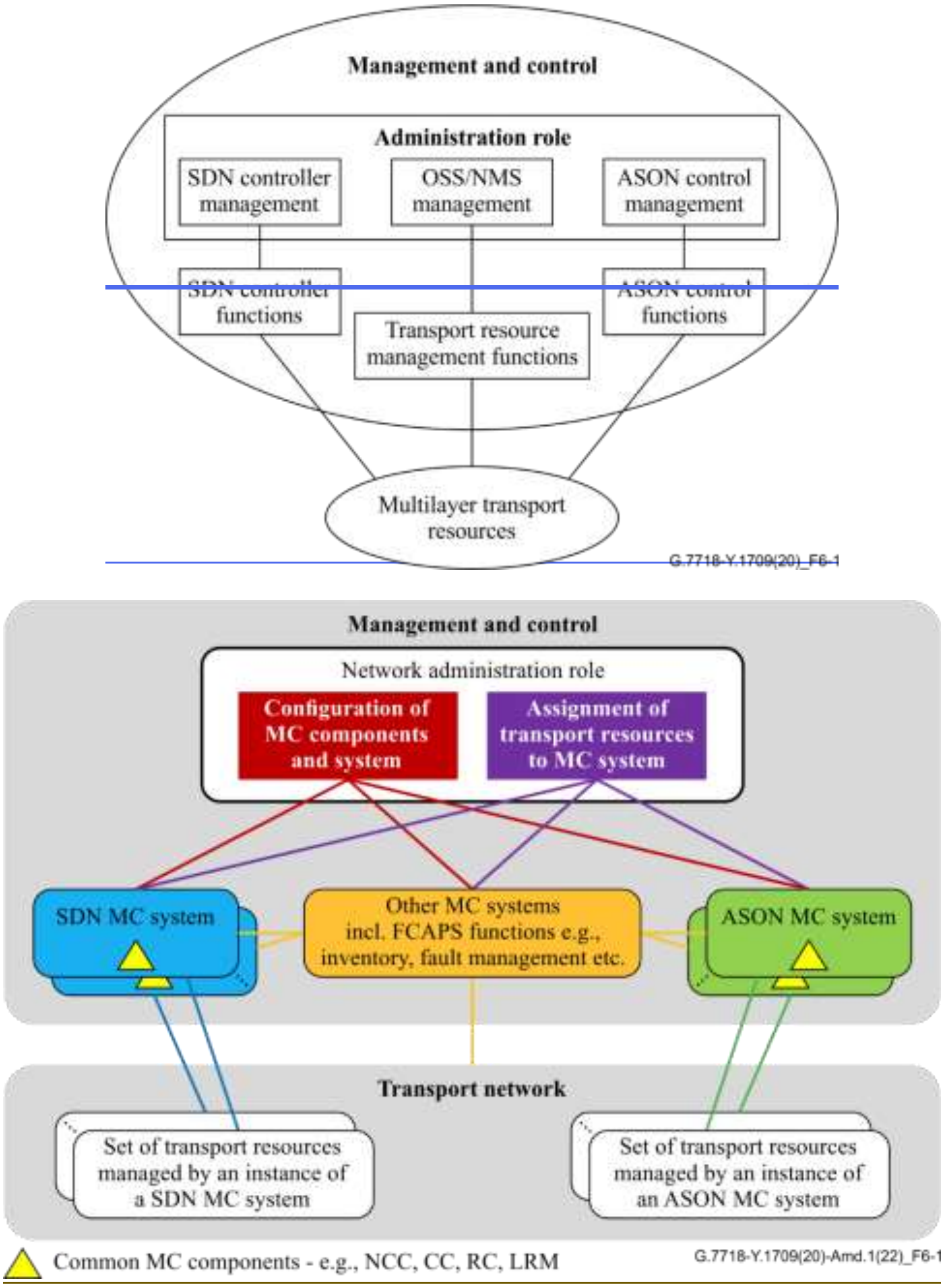


Figure 6-1 – Management-control continuum (from Figure 6-1 of [ITU-T G.7701])

The administration role manages the MC functions or system. It does not directly manage the physical or abstracted transport resources. The management functions performed by the administration role would include the resource allocation for each client context, the policy configuration of the MC components, the DCN configuration and security related configurations for the MC functions, etc. The administration role and associated management functions are essential for management and control system.

6.2 MC system/component/function

A management and control system (MCS) is composed of a set of management and control components. The MC components interact with each other to perform the management and control functions, which then manage and/or control the transport network resources. The MCS could be standalone element management system/network management system/software-defined networking (EMS/NMS/SDN) controllers, or ASON control, or system with integrated management and control functions.

MC component is an abstract representation of an MC functional entity. In this Recommendation, MC components do not represent instances of implementation code. They are used to construct scenarios to explain the operation of the architecture of managing MC functions and components.

Transport MC functions operate on transport resources and receive state information about the resources. Transport MC components and functions for control purposes are defined in [ITU-T G.7701], [ITU-T G.7702] and [ITU-T G.~~8080~~7703]. Transport MC components and functions for management purpose are defined in [ITU-T G.7710].

The relationship between MCS, MC component, MC function and network resource is shown in Figure 6-2 below.

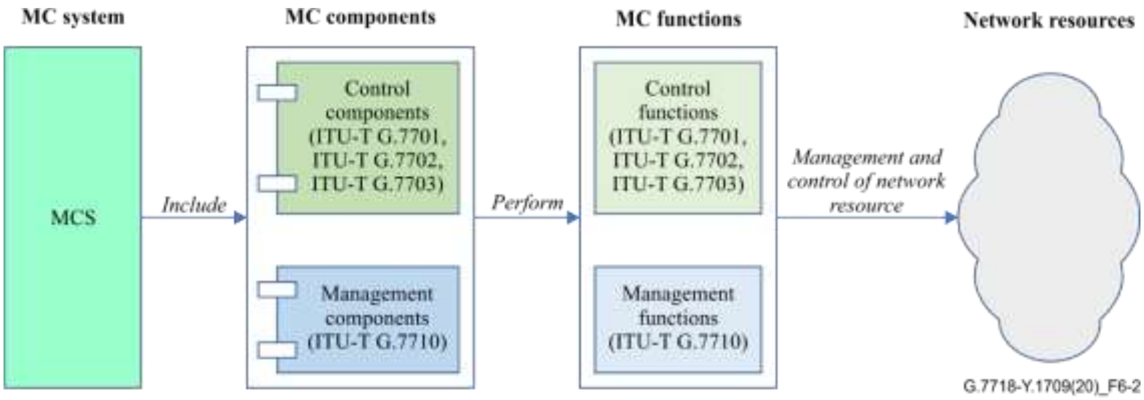


Figure 6-2 – Relationship of system, component, function and network resource

6.3 Management of MC components and function

As outlined in clause 1, the MC components and functions also require management. In the current edition of this Recommendation, only the management requirements of the MC components/functions defined in [ITU-T G.7701], [ITU-T G.7702] and [ITU-T G.~~8080~~7703] are described, the scope of this current edition is shown in Figure 6-3. The management requirements for MC components/functions in other specific MCS is implementation related and are outside the scope of this Recommendation.

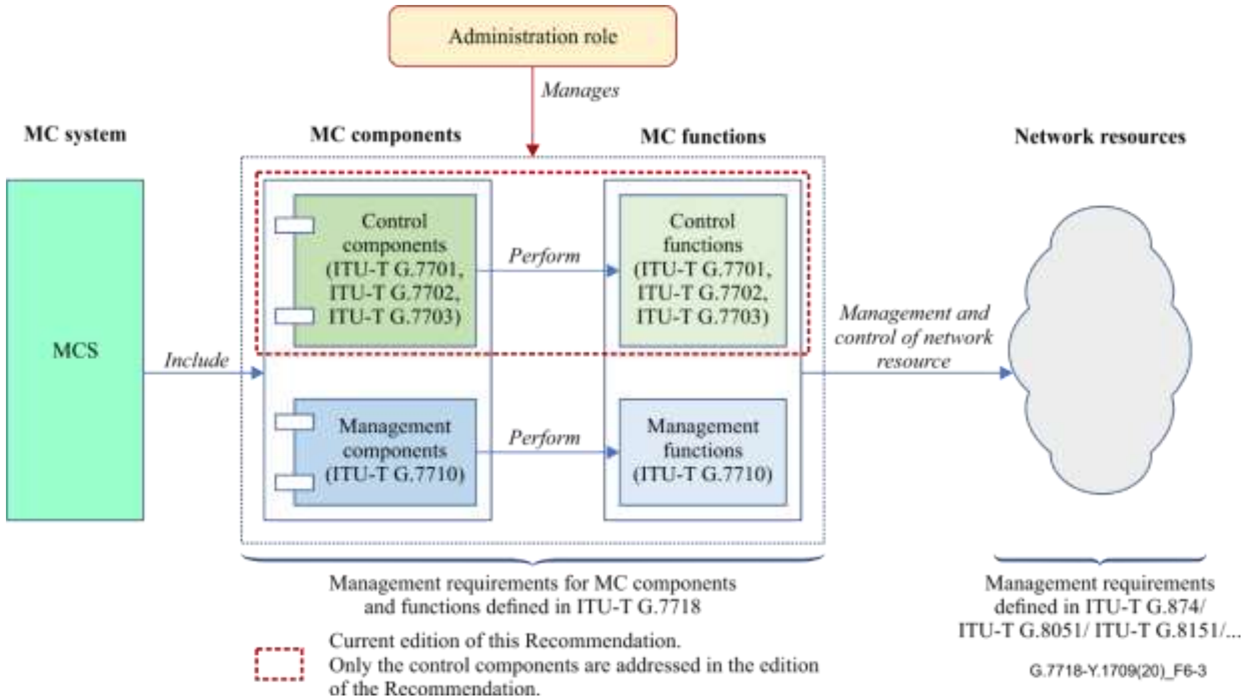


Figure 6-3 – Management of MC components and functions

6.4 DCN aspects

To enable management and control components to communicate with each other, the data communications network (DCN) is used. DCN identifiers are the point of attachment of the DCN to the protocol controller. Several PCs may share a DCN point of attachment and any given NE may have multiple points of attachment. [ITU-T G.7712] contains the specifications for the use of DCN to support management and control communications. The connection of MC component and network element through DCN is shown in Figure 6-4.

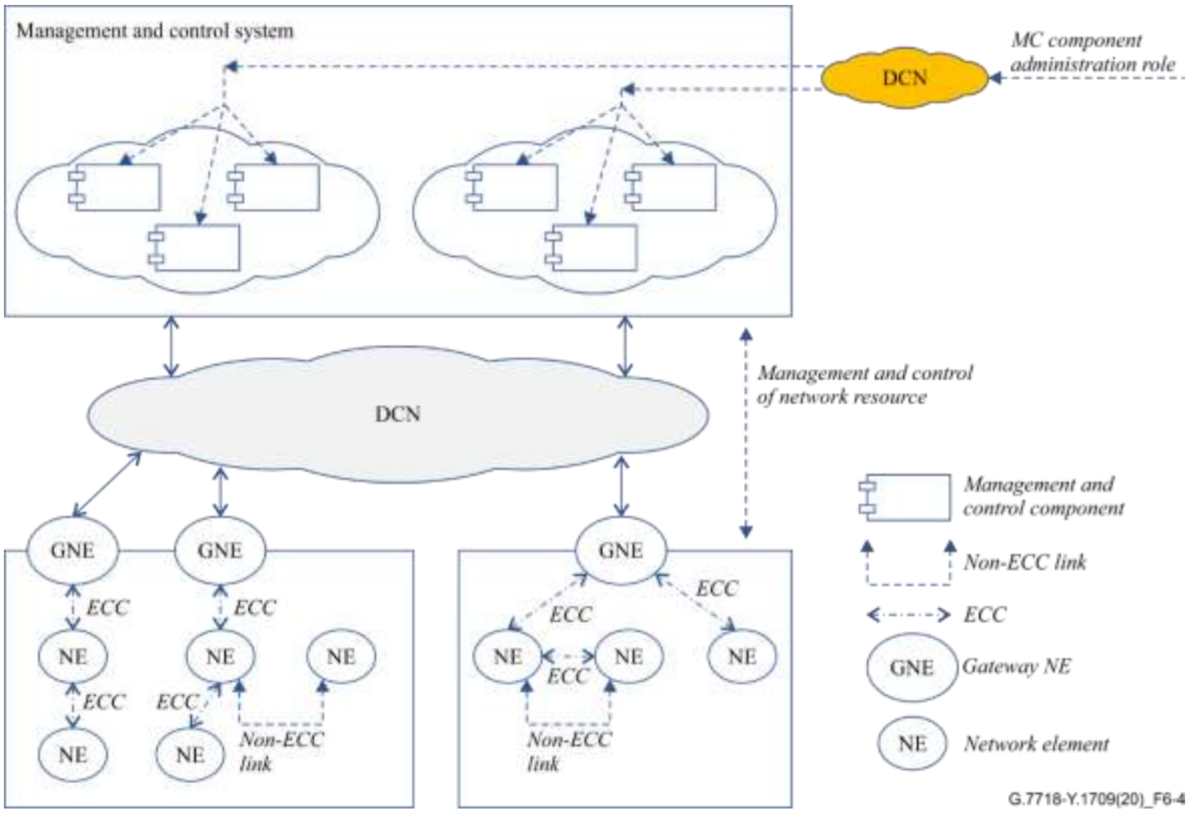


Figure 6-4 – DCN aspect in the MCS management

6.5 Management aspects

6.5.1 Overview of management requirements of MC components/functions

The management of MC components, which include the management of components to manage the transport resources and the control functions, is part of the MC functions as shown in Figure 6-2 of [ITU-T G.7701], MC components themselves need to be managed/controlled to fulfil their responsibility. The management requirements of MC components/functions include fault management, configuration management, account management, performance management and security management. For example, the identifiers and DCN addresses of the protocol controller components need to be configured before they can communicate with each other. The performance of each component needs to be monitored to make sure there is no bottleneck in any component, security management is mandatory for the controller which provides service to other client controllers.

The management aspects in this Recommendation also cover lifecycle management of transport resource and MC components. For the MC components, they need to be created/destroyed whenever a new client controller is connected/disconnected to/from a server controller. The lifecycle management of transport services and/or resource is also within the scope of this Recommendation.

6.5.2 Component interface and context

MC components interwork with other MC components. The interfaces of MC components are defined in [ITU-T G.7701], [ITU-T G.7702] and [ITU-T G.~~8080~~7703]. In [ITU-T G.7711], ControlConstruct object class is defined to model the control functions. ConstraintDomain object class is used for the control scope representation and ExposureContext instance defines what can be accessed through a particular ControlPort and who can have access across the client/server boundary. The control context represents a view of the things controlled by a control system. Detail management requirements of context are specified in clause 9.

6.5.2.1 Client context

According to the description in clause 6.~~2~~4 of [ITU-T G.7702], client context within an SDN controller is a set of information used to support a particular client, which include, for example a virtual network (VN), as well as the management-control functions created for that client.

Client context need to be created before interacting with upper level server context. Detail management requirements for client context are defined in clause 9.

6.5.2.2 Server context

According to the description in clause 6.~~2~~4 of [ITU-T G.7702], when a server is used by an SDN controller, that SDN controller is supported by a set of information relating to that server as well as management-control functions and this is known as the server context.

Server context need to be created before interacting with the lower level client context and/or ~~physical~~ local resources. Detail management requirements for server context are defined in clause 9.

6.5.2.3 Administrative context

Administrative context is a set of information used by administration role, it is created at the time the controller is launched, it has unrestricted visibility and authority to perform all kinds of operations on its resource. Administration role can create additional client context for each of its clients according to the contract/parameters negotiated between administrator and each client, which may include route information like constraints, policy, and resiliency information among different virtual ports.

Administrator can also create additional server context for each of its server controllers according to the contract/parameters negotiated between administrator and each server controller, which may include the same information as with its client.

6.5.3 Overview of control and management model

Annex H of [ITU-T G.7711] defines the control model by following the component-system pattern (see Appendix V of [ITU-T G.7711]). In the component-system pattern, a component could be an encapsulation of a system and provide an abstract/opaque external view for hiding the system details. Components could be interconnected to form a higher-level system. MCS functions could be decomposed into MC components; MC components may talk to other MC components about the resource they are managing-controlling.

In [ITU-T G.7711], several control-related model artefacts (object classes) have been defined. The object class of ControlConstruct is defined to represent the control and management capability/functionality. It processes information to control other functions (such as ProcessingConstructs, Forwarding constructs etc.). The ExposureContext object class represent a view of the things controlled by an MCS. The ConstraintDomain object class represents the control scope. Both the management and control cases such as control functions inside network element, SDN controller, EMS/NMS could be represented by ControlConstruct object class. A ControlConstruct instance communicates with other ControlConstruct instance through ControlPorts about things within the related ConstraintDomain. Together with the aforementioned object class, ControlPort, CdPort and VmfPort object classes are defined to follow the component and port pattern as described in [ITU-T G.7711].

This Recommendation defines the management requirement for the components defined in [ITU-T G.7701], [ITU-T G.7702] and [ITU-T G.~~8080~~7703]. The ITU-T G.7711/Y.1702 core information model could be used as the base for defining the information model, through pruning and refactoring and extension, for managing the components according to requirements of this Recommendation.

7 Transport resource identification and allocation

7.1 Transport resource identifiers

7.1.1 Physical resource and virtual resource

[ITU-T G.7711] defines the generic protocol-neutral information model for transport resources, in its Annex F, models for physical equipment such as cable and connector were defined. These object classes are used to represent the truly physical equipment and resource.

For the other transport resource represented by the information models, it could be partitioned among different MC instances. Virtualization process realized by MC components create an abstraction and subset of resource whose selection criterion is dedication of resources to a particular client or application. Transport resources may be used to provide service for multiple clients under the management/control of MC components. In the multi-level controller architecture, the resource in the server context of the client controller is a virtualization of resource in the client context of server controllers.

Management and control functions may have the same view for the network resource except they may use identifiers from different name spaces for identifying the resource.

7.1.2 Resource identifier

Transport resource need identifiers in different namespace. Interactions between identifier namespaces must be considered for OAM functions and protocol controller design.

– Identifier of transport resources within a layer network

  Applications that control, use or observe the transport network need the ability to identify some entities within the transport network. Each of these applications requires an identifier for each of the transport network entities that are of interest. To allow the network to be configured to support multiple communications that are delivered to only the intended receiver(s), the configuration application and the layer network must be able to distinguish the topological components, the resources and the individual communications. Annex A.4 of [ITU-T G.800] describes for this purpose the following identifiers:

  – Access point identifier
  – Connectivity label
  – Resource label (Note that the resource label is frequently used as the identifier for the Forwarding point (FP))
  – Forwarding end port (FEPt) identifier
  – Forwarding port identifier
  – Forwarding identifier
  – Link point identifier
  – Subnetwork identifier

– Identifier of transport resources in control view

  [ITU-T G.7701] control components use three different name spaces to identify the transport resources:

  – Routing area name space and subnetwork name space provide identifiers for [ITU-T G.800] topological entities (subnetworks and links).
  – Link context name space that provides the identifiers (SNPs) for the ends of transport entities ([ITU T G.800] FPs).

– FP name space used by the TAP and DA to directly configure forwarding in transport entities. The TAP and DA provide a mapping between the SNP identifier and the forwarding resource identifier.

– Identifier of transport resources in management view

Management information models, such as [ITU-T G.875] and [ITU-T G.7711] define model artifacts to represent the transport resources, entities, and topological components. Examples artifacts are trail termination point (TTP), connection termination point (CTP), logical termination point (LTP), forwarding domain (FD), link, and forwarding construct (FC). Identifiers for identifying these model artifacts are defined in the models as attributes. Figure 7-1 shows the mapping between the model artifacts and the transport entities, and the mapping between the model artifacts in the model evolution.

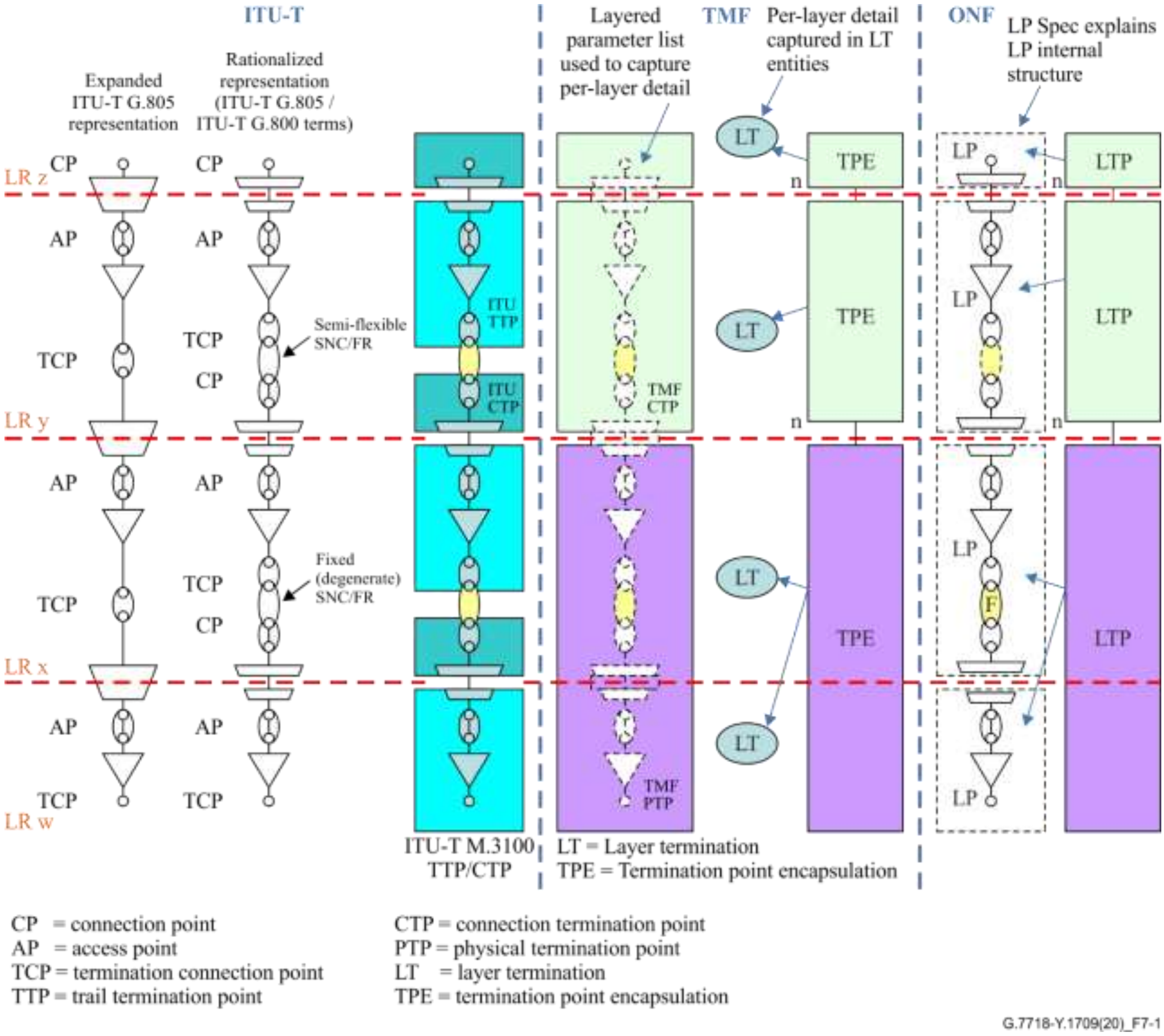


Figure 7-1 – Mapping from ITU-T and TM forum termination models to the core

(source: Figure B.2-9 of [ITU-T G.7711])

MCS SHOULD support the assignment of identifiers for management and control objects in related identifier spaces, e.g., RA identifiers, SNPP identifiers, UNI/E-NNI transport resource identifiers in ASON, etc.

MCS SHALL support the administration of identifiers including ensuring their uniqueness within their respective spaces. It SHALL be possible to locate resources in one namespace, and to navigate to the same resource from the other namespace.

MCS SHALL support the ability to configure the binding and retrieve the relationship of a transport resource identifier between different namespaces.

The identity of CTP link connections in [ITU-T G.800] forwarding point (FP)~~physical transport resource~~ name space could be provided to the control and management functions.

ASON UNI/E-NNI transport resource identifiers could be assigned per individual carrier's specifications.

7.2 Transport resource allocation

Clause 6 of [ITU-T G.7701] gives an overview of the resource partition among MC instances, network resources MAY be partitioned among those under the authority of management systems, those under the authority of the SDN controllers, and those under the authority of the ASON control.

Clause 6 of [ITU-T G.7702] describes the process of network resource assignment and allocation between server contexts and client contexts by the administration role during the process of network virtualization.

The administration role as shown in Figure 6-3 take the responsibility of resource partition and allocation within MCS.

The administration role SHALL support the determination of a resource's partition and assignment, i.e., assignment of being controlled by control functions or being managed by management functions.

It SHALL be possible to locate the resources of being controlled by control functions and resource being managed by management functions, i.e., the resource in administrative context or ASON/SDN control context, and to navigate to the same resource between management and control functions.

The administration role SHALL support the allocation of transport resources, e.g., CTPs, to be controlled by the control functions, allocation of flexible adaptation resources should also be supported. Only one SNP in each SNPP can be associated with a CTP. Multiple SNPs (in different SNPPs) can be associated with a single CTP.

The administration role SHALL support the ability to either assign or remove resources to/from the control functions. When the transport resources are not being used to support any existing connections/connection segments, they can be moved from administrative context to ASON/SDN control context or vice versa. Other scenarios, including the migration from administrative context to ASON/SDN control context or vice versa, require further study.

The administration role SHALL support the ability to shut down specified transport resources. See also [ITU-T X.731] for the definition of "shutting down" state.

The view of topology in administrative context SHALL be independent of the control scenario and protocol choice. It should be noted that the format of the topology objects for ASON is defined in Recommendations that address ASON information object specifications.

8 Management requirements of MC components and functions

The basic methodology of describing transport network functionality of network elements is defined in [ITU-T G.806]. In this Recommendation, a unified methodology and architecture is used for describing the management requirements for MC components and functions. They are similar to the functional blocks-based management requirements definition methodology used in [ITU-T G.874], which describes the management requirements of equipment functional blocks defined in [ITU-T G.798] for optical transport network (OTN).

The original requirements have been analysed and categorized as shown in Appendix I in this Recommendation. The original requirements have been categorized into FCAPS function domains as defined in [ITU-T X.700] and allocated to different MC components. The categorized requirements in Appendix I are summarized in this clause for each component.

MCS support the management of MC components with different distribution of implementation (centralized versus fully or partially distributed), MC system SHALL support both centralized and distributed implementation of the MC components. The information model of MC components defined in [ITU-T G.7719] supports both centralized and distributed management of MC components.

MCS SHOULD support the identification of inconsistencies between databases in management and control functions and synchronize the inconsistencies. Notifications SHOULD be generated if there's inconsistencies between management and control functions.

8.1 Lifecycle management requirements of the MC components/functions

MC components and the exposed context have its lifecycle which need to be managed, this kind of lifecycle is different from the lifecycle stereotype associated with object classes which indicate the maturity of object class in the information model.

The basic CRUD (Create/Read/Update/Delete) style operations are applicable for both MC components and context. The CRUD style operation of MC components ~~is~~ could be used to build the ControlConstructs for interaction with other controllers. The interactions of MC components between controllers are subject to the accessing rules defined in the ExposureContext.

Create/Read/Update/Delete of MC component SHOULD be notified to the MC management functions.

The upgrade of MC components in the MC system SHALL not affect configured services in the transport network.

As mentioned in clause 6.4, client/server contexts are created for interaction with adjacent level controllers. The administrative context server as a default context is created when the controller is launched, through this context, it supports the CRUD style operation of more client/server contexts and MC components. When the context for a client or server controller is deleted, its associations with resources and affiliated management and control information such as the routing information for this context should be deleted.

8.2 Configuration management requirements of the MC components/functions

MC components require separate name spaces, and they may be instantiated differently from each other for a given control function instance. For example, one can have centralized routing with distributed signalling. Separate identifiers are thus needed for:

– routing controllers (RCs);

– network call controllers (NCCs);

– connection controllers (CCs).

Additionally, MC component such as protocol controllers (PCs) are used for protocol specific communication. These also have identifiers that are separate from the (abstract) components, e.g., RCs.

The individual MC components SHALL support the configuration of parameters, a mechanism for detecting inconsistent settings for the parameters SHALL be provided.

In SDN MC system, domain division is mostly based on control requirements. For the transport network, it could be divided by the network resources of different equipment manufacturers. It could also be divided by different layers. In ASON MC system, domains are usually divided according to distributed requirements.

From the perspective of management or/and control purpose, the domain could have special functions with managerial and/or policy considerations, and inherent transport network heterogeneity (including control and management). Typical domains include administrative domain, control domain, routing domain, recovery domain, etc. A domain centralizes the MC components that accomplish a specific purpose and the resources that need to be implemented for that purpose.

From the perspective of context view, it is necessary to divide the administrative domain within the scope of the administrative context. The domain is configured according to the management requirements and used to interact with managers in management functions.

For clients, it is necessary to divide the control domain corresponding to the client context, which covers the MC components and control resources that provide services to clients. The MC components interact with clients through the boundary interface of domain.

For server, the control domain corresponding to the server context needs to be divided.

A control domain provides an architectural construct that encapsulates and hides the detail of an implementation of a particular group of MC components of one or more types. MC component supports publishing interface capabilities to domains boundary. The control domain SHALL support configuring the ability to capture the interaction information of interfaces in the domain as the information basis for the interaction between control domains.

MC components need to support the configuration of domain identity. For the same domain, the domain identity of MC components should be unique, and the namespace should be consistent. Different MC systems and different layered architectures have different domain configuration information. And the way of domain division is different from different dimensions.

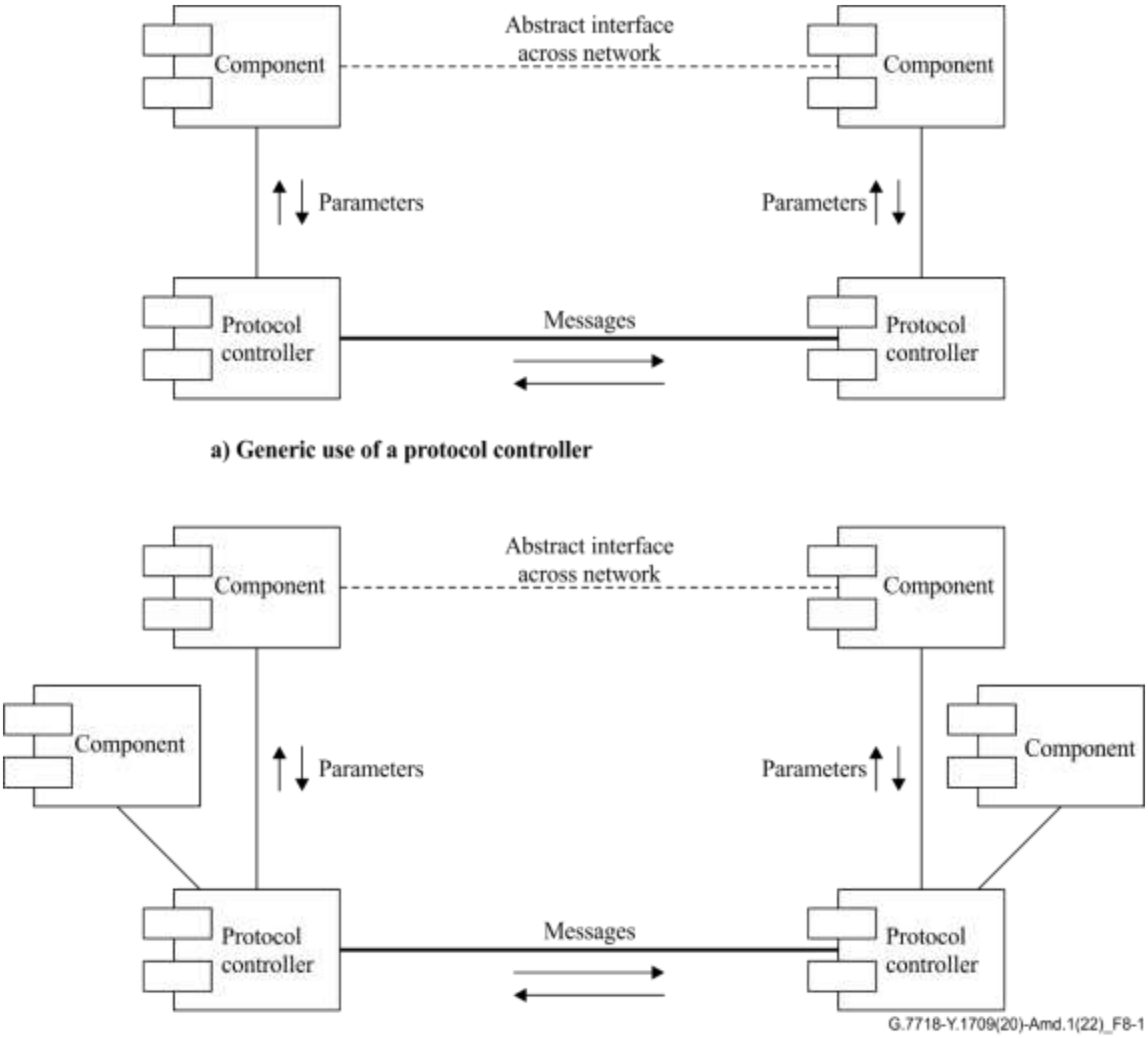
8.2.1 Protocol controller (PC) component

The protocol controller maps the parameters from one or more ~~of the abstract~~ interfaces of the control components into messages that are carried across the CCN. It also demultiplexes messages received from the CCN into parameters that are passed to other MC components.~~by a protocol to support interconnection via an interface~~.

The protocol controller maps the parameters from the interfaces of the control components in the same MC system into (external) messages that are carried by a protocol to support interconnection via an external interface.

Parameters are passed between MC components in different MC systems via the protocol controller. The protocol controller is semantically transparent to parameters being passed. The parameters are mapped into external protocol messages and vice versa. Messages are passed between the two protocol controllers.

Figure 8-0 gives a general description of the protocol controller component.



b) Generic multiplexing of different primitive streams into a single protocol

Figure 8-0 – Protocol controller component

(source: Figure 8-19 of [ITU-T G.7701])

Interactions between components through protocol components, the status of protocol control components SHOULD not impact operation and configuration of its controller or management components.

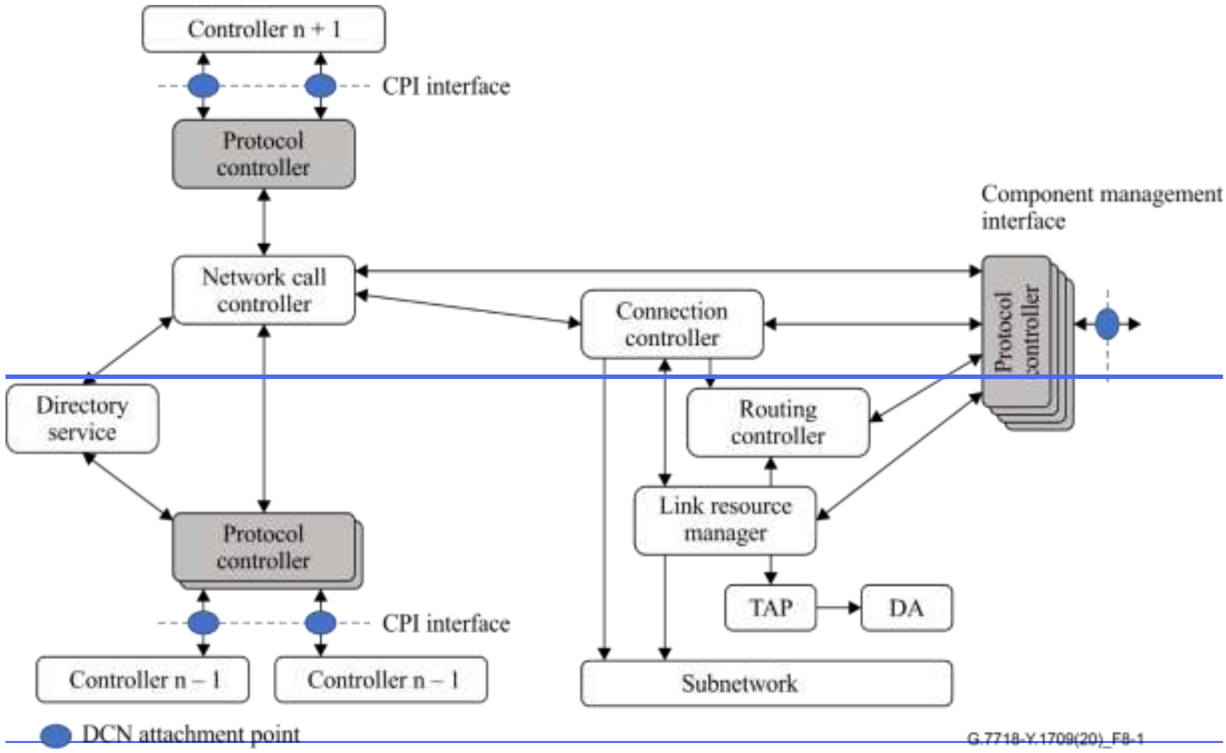
The PC component can be configured on a per interface or per group of interfaces basis. The configuration of protocol controller SHOULD support the configuration of specific protocol for each controller among the protocols supported by a given system (specific protocol aspects are outside the scope of this Recommendation).

The PC component SHALL support the configuration of policy parameters and querying of policy parameters.

Point of attachment to the DCN SHOULD be configured and the address for each protocol controller SHOULD be assigned by the management function.

The PC component SHALL support the configuration of unique identifiers for their points of attachment to the ~~D~~CCN.

The configuration of the binding of the control components (e.g., CC) to the PC component SHALL be configured. Multiple protocol controllers MAY share the same point of attachment to the ~~D~~CCN. A network element MAY have multiple points of attachment to the ~~D~~CCN. The attachment of PC to ~~D~~CCN is shown in Figure 8-1.



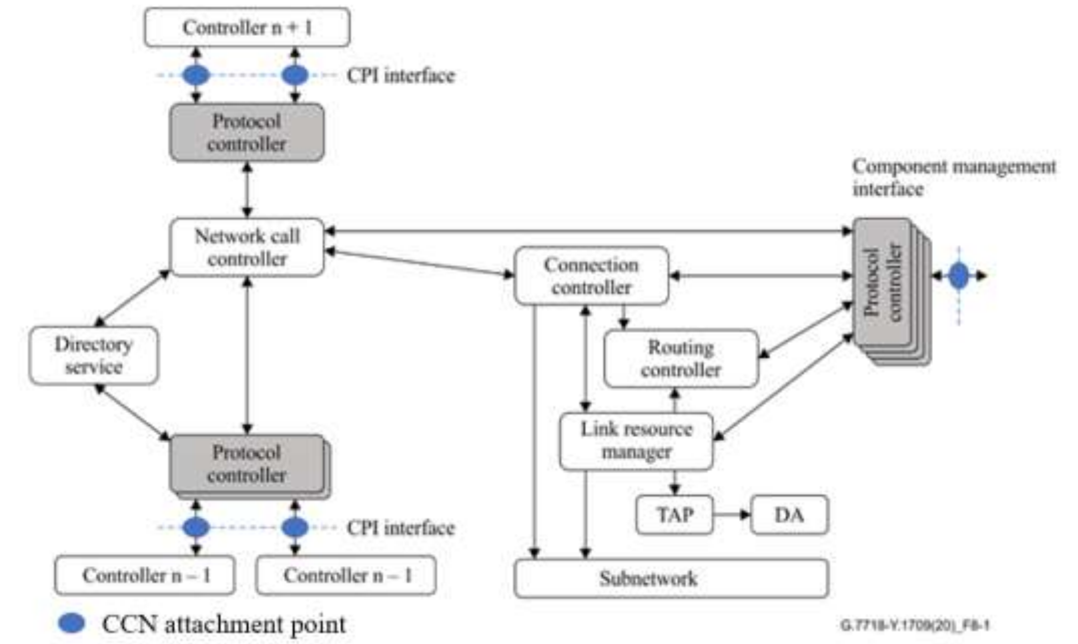


Figure 8-1 – PC binds MC components and one or more point of attachments

The PC component SHALL support the configuration of the parameters for individual control and management components. A mechanism for detecting inconsistent settings for the parameters SHALL be provided.

In ASON case, the specific protocol(s) selected for individual protocol controller SHALL be specified as follows:

a) UNI signalling protocol;

b) UNI discovery protocol;

c) E-NNI signalling protocol;

d) E-NNI routing protocol (if multiple protocols are supported);

e) E-NNI discovery protocol;

f) optionally I-NNI signalling protocol;

g) optionally I-NNI routing protocol;

h) optionally I-NNI discovery protocol.

In the distributed network control mode of ASON case, The PC component SHALL provide support for each SNPP, the configuration of the control function is required to create/delete/modify the following interfaces: UNI, I-NNI and E-NNI. PC shall also support the configuration of the parameters necessary for UNI signalling, I-NNI signalling, and E-NNI signalling. A mechanism for detecting inconsistent settings for these parameters shall be provided. The specific parameters are defined in the relevant standards, including [ITU-T G.7713.1], [ITU-T G.7713.2], and [ITU-T G.7713.3]

In logically centralized network control mode as SDN controller, The PC component SHALL support the configuration of the parameters necessary for the control plane interface (CPI).

8.2.2 Call controller component

The call controller components SHALL support the retrieval of call attributes including call name, calling/called transport resource identifiers, class of service (CoS) and grade of service (GoS) by the management functions. The call controller component SHALL also support the retrieval of call start and end times, and associated connections by the management functions.

The call controller components SHALL support the ability to manage calls with zero or more connections. For each call, the call controller SHALL support the ability to be configured to add, remove, or modify a connection.

The call controller components SHALL support the ability to refresh the MC components with changes that have occurred as a result of call modification. This includes increasing/decreasing the bandwidth of an existing connection, increasing/decreasing the number of connections associated with the call, or increasing/decreasing the size of an inverse multiplexing group.

The call controller components SHALL support the retrieval of call attributes including call name, calling/called transport resource identifiers, CoS and GoS by the management functions. The call controller shall also support the retrieval of call start and end times, and associated connections by the management functions.

The call controller components SHALL support notifications to the management functions of any defects associated with a call release request.

The call controller components SHALL support call request success indication to the management functions. The call controller component SHALL support call request failure indications with a code identifying the reason for the failure.

ASON call controller must support the capability to distinguish a soft permanent connection (SPC) from an SC. This is done via a call attribute that distinguishes the party responsible for end point handling of the call (i.e., whether the calling/called party call controller is at the UNI or the MC system).

8.2.3 Directory service component (DS)

The directory service component is responsible for identifier resolution and coordination among peer directory service components. This component provides mappings between identifier spaces for other components.

The DS component SHALL support to be configured with the binding, and retrieve the relationship, of transport resource identifiers in different namespaces.

The DS component SHALL support the configuration of a specific SNP. The information to be configured for the SNPP members include the relationship between SNP and CTP.

NOTE – The lower order part of the SNP identifier may either be provided or auto-generated from the lower order part of the CTP name (i.e., time slot).

8.2.4 Termination and adaptation performers (TAP)

The TAP components allocate labels for transport resource, binds labels to SNP identifier and provides view for the link resource manager (LRM). It hides any hardware and technology with specific details of the adaptation and termination control.

The TAP SHALL support the capability of assigning all CTP link connections in one trail to one SNPP link in one operation. TAP SHALL also support the capability of binding SNPs to CTPs without having to manually provision each binding.

TAP component SHALL support the configuration of FEF information from LRM, which is used to establish FEF fault events list and filter fault events.

8.2.5 Link resource manager (LRM) component

The LRM components are responsible for the management of an SNPP link; including the assignment and unassignment of SNP link connections (to a connection), managing resource reservation, configuration of policing and shaping functions (if required), providing topology and status information [ITU-T G.~~8080~~7703].

The LRM component SHALL support the configuration of a specific SNP. The information to be configured for the SNPP members include the SNP parameters such as SNP states as not validated, shared, etc.

The LRM component SHALL support the ability to define one or more shared risk groups (SRG), a link could be provisioned to belong to multiple SRGs.

The LRM component SHALL support the configuration of SNPP links which will include at least the provisioning of routing area information. The LRM component SHALL allow the configuration of the SNPP link parameters needed for routing, signalling and management (name, directionality, cost, etc.).

The LRM component SHALL all allow single-ended SNPP link provisioning. Note that for this case, initial provisioning of the subnetwork names and SNPP name must be done at both ends.

The LRM component SHALL support the configuration of notifications for the discovery of any changes to the intra-domain topology and inter-domain topology.

The LRM component SHALL support the configuration of FEF information from CC to help the rapid recovery of affected connections in the MC system, and allow the same value setting and/or recursive decomposition setting of FEF information in multi-level MC system.

8.2.6 Routing controller (RC) component

The routing controller (RC) component is mainly responsible for topology query of management purposes, route configurations and route computing request of setting up connections.

The RC component SHOULD have the capability to support the configuration of parameters required for diverse routing.

The RC component SHALL have the capability to support transferring of routing information with other MC components.

The RC component SHOULD support the query of topological information and should support the maintenance of hierarchical inter-domain topology information.

The RC component SHOULD support routing area aggregation and disaggregation configuration, RC adjacencies configured by management function should be supported.

In the case of ASON, the RC component could be assigned to a particular routing area and routing level in a hierarchical routing architecture. This configuration could be reconfigured.

The RC component SHALL support the configuration of the parameters necessary for I-NNI routing and E-NNI routing in ASON application. The ASON routing architecture and requirements are defined in [ITU-T G.7715] and [ITU-T G.7715.1]. A mechanism for detecting inconsistent settings for these parameters, e.g., timers, shall be provided.

8.2.7 Connection controller (CC) component

The CC component SHALL support the capability to specify the explicit resource list for the management function initiated connection set-up request. The explicit resource list is defined in clause 7.2.3.3 of [ITU-T G.7713].

The CC component SHALL support the ability to initiate control functions directed maintenance rollovers.

A code identifying the reason for the failure in the connection request SHOULD be reported to the management functions by the connection controller.

Indications of a successful connection creation SHOULD be notified to the management functions; the notification SHALL contain sufficient information to permit correlation with other connection segments.

Indications of successful connection re-route or failure of connection re-route SHOULD be reported to the management functions by the connection controller. A code identifying the reason for the failure in the re-route SHOULD be reported.

Status of all connections and the value of connection attributes SHOULD be reported by the connection controller to the management functions.

The CC component SHALL support queries of all relevant attributes of the control function controlled protected connections by the management functions.

The CC component SHALL support the configuration of all relevant functions of the control function controlled protected connections.

The CC component SHALL support the selection of the reversion process to be used with re-routed connections, e.g., manual or automatic reversion.

The CC component SHALL support notifications of a service restoration failure.

The CC component SHALL support the provisioning of timers (e.g., revert and restore) per re-routing domain.

Three types of connection establishment are defined in [ITU-T G.~~8080~~7703] as permanent connection, switched connection (SC) and soft permanent connection (SPC), SC and SPC are created with ASON control functions, the following requirements are needed for SPC and SC:

1) The CC component SHALL support the ability to manage soft permanent connections, including those that make use of VCAT and LCAS functions. Specifically, the following SHALL be supported:
   a) The ability to invoke the set-up of a soft permanent connection.
   b) The ability to invoke the release of a soft permanent connection.
   c) The ability to invoke the modify operation of a soft permanent connection.
   d) The ability to invoke the re-routing of a soft permanent connection.
   e) The ability to query the control functions for the status of a soft permanent connection.

f) The ability to query the control functions for the connection attributes of a soft permanent connection including route information.

g) The ability to allow the management functions to request a VCAT SPC with different service levels (making use of diverse routing of bundles).

h) The ability to allow the management functions to modify SPCs which make use of the VCAT and LCAS functions, i.e., to increase or decrease the bandwidth without service interruption.

i) The ability to support the provisioning of class of service parameters, which may be mapped to protection/restoration mechanisms and configurations within the networks.

2) The CC component SHALL support requests for migration from a PC to a SPC. The transport resource supporting the PC should be moved from the scope of managed by the management function to the scope of control function without service disruption. A call with the appropriate parameters (including state information) shall be created such that the ASON control functions can manage the call.

3) The CC component SHALL support the ability to specify an SPC using class of service parameters which may be mapped to constraint-based routing. This may include, but are not limited to link, node and SRG diversity.

4) The CC component SHALL support requests for switched connections (SC). This support SHALL include:

a) Notifications of the set-up, release, and modification of SCs.

b) The ability to invoke the release of an SC.

c) The ability to invoke the re-routing of an SC.

d) The ability to query the control functions for the status of an SC.

e) The ability to query the control functions for the connection attributes of an SC including route information.

f) The ability to support the provisioning of class of service parameters, which may be mapped to protection/restoration mechanisms and configurations within the networks.

5) The CC component SHALL support the exchange of information pertaining to switched connections created in the network.

NOTE – [ITU-T G.7713] and the ITU-T G.7713.x-series of Recommendations contain specific information on connection attributes.

8.2.8 Discovery agent (DA) component

Network elements supporting automatic discovery SHALL support a management information base for all discovered resources.

8.2.9 Notification component

Clause 8.2.8 of [ITU-T G.7701] describes the functions of notification control component, it leads to the following requirements:

The notification component SHALL support the configuration of subscriptions for notifications.

The notification component SHALL support the query of subscriptions and query of history notifications that have been subscribed.

The notification component SHALL support the configuration of parameters for alarm correlation.

8.3 Fault management requirements of the MC components/functions

MC component and functions SHALL support the configuration of alarm characteristics. MC component and functions SHALL support autonomous alarm notification from each component and function for each fault. Information in the notification SHALL include the resource in alarm, the time the alarm occurred, the probable cause, and the perceived severity of the alarm. MC component SHALL support the ability to query all or a subset of the currently active alarms. MC component and functions SHALL support administration of alarm severity in accordance with the TMN requirements specified in [ITU-T M.3100] and [ITU-T M.3120].

MC component and functions SHALL support querying of the operational state of MC components.

A failure in MC components SHALL neither affect the normal operation of a configured transport resource, nor the status of configured connectivity services in the transport network. A failure of an MC component SHALL not affect the normal operation of other components. The failure and recovery of interfaces between any MC components SHALL be detected.

8.3.1 Protocol controller (PC) component

Control components access the CCN via a PC, the PC component SHALL support the capacity of detecting and reporting the failure of its DCN connection with peer part to management functions.

8.3.2 Discovery agent (DA) component

Discovery agent component in ASON application SHOULD support notification of failures in the link capability exchange procedure. The notification shall indicate the reason for the failure.

Discovery agent component in ASON application SHOULD support notifications of a successful link capability exchange procedure, the notifications shall include service attributes for the ASON UNI-C and UNI-N ports.

8.4 Performance management requirements of the MC components/functions

MC component and functions SHALL support collection of the necessary current and historic usage data, such as call attempts, call set-up failures including reasons and successes. The data should be available upon the query from the MC system.

MC component and functions SHALL support the ability to query current and historic performance data.

Specific performance parameters for MC components and functions are for further study. A possible parameter is the number of connection re-routing events per call.

MC component and functions SHALL support an appropriate notification of failed connection set-ups, failed connection re-routes, etc., that exceed a configured threshold.

8.4.1 Link resource manager (LRM) component

LRM SHALL support the ability to retrieve SNPP link usage information from the control functions.

8.4.2 Connection controller (CC) component

CC component and functions SHALL support queries of the connection attempts, connection set-up failures and successes.

8.5 Accounting management requirements of the MC components/functions

This Recommendation is limited to the representation, storage and communication of data associated with call details.

The call control component SHALL support the capability of querying of a batch of call detail records. Call details record SHALL be available after a call terminated, call details record SHALL include attributes such as customer identification, call start time, call end time, bandwidth, grade of service, and call type (i.e., SPC/SC in ASON, point to point connection or VN service in SDN).

9 Context management

9.1 Context lifecycle management

9.1.1 Context creation management

The procedures for the creation of an administrator ~~client~~ context that has unrestricted visibility and authority to perform all kinds of operation formed at the time of the launch of MCS is discussed in clause ~~6.6.1~~7.4 of [ITU-T G.7702]. The administrator then creates a client context for each of its clients. From the aspect of context lifecycle, this is the management activity for client context creation, so it is extended here to the management requirements of client context creation.

Client contexts ~~shall~~ SHALL be created ~~for their~~~~by the~~ as a result of the requests from external clients and ~~supported clients according to~~ the contract/parameters negotiated between MCS administrator and the clients.

The server context SHALL be created by the administrator for each of its server controllers according to the contract/parameters negotiated between the administrator and each server controller. The server context may also be created by the administrator for the local resources. The administrator could access the local resources or interact with the lower-level client context through the created server context.

9.1.2 Context deletion management

The client contexts SHALL be deleted as clients cancels the association ~~contract~~ with the server controller~~administrator~~.

The administrator SHALL have the ability to delete client contexts.

Virtual network resources are provided to the client in the client context. When the client context is deleted, the virtual resources and resource mapping SHALL be released together. This situation is described in clause ~~10~~15.1.2 of [ITU-T G.7702], including the processes of the delete operation.

When a client context is deleted, the VN dedicated to that client SHALL be deleted, and the corresponding SNPs and/or FPs in the transport resources shall be released.

9.1.3 Context modification management

The client contexts SHALL support~~be~~ update operations executed~~d~~ by~~for~~ ~~their~~ the administrator ~~supported clients~~ based on changes in the contract/parameters negotiated between administrator and the clients.

Examples of modification include modification of security settings for authentication, authorization, etc., for a client context accessing from the client.

The server contexts SHALL support update operations executed by the administrator based on changes in the contract/parameters negotiated between administrator and the client.

9.1.4 Context retrieval management

Client contexts SHOULD support retrieval ~~operations from~~by the clients/administrator based on requirement management.

Server contexts SHOULD support retrieval by the administrator based on requirement management.

9.2 Context's support of resource configuration

The configuration and update of resources in the client context by the client are realized by cross contexts interaction between the controller and its client controller. The related management requirements of context, context and interaction between components will be reflected in different application scenarios, e.g., resource virtualization that is mentioned in clause 7.46.6.1 of [ITU-T G.7702].

Server contexts SHALL support request for configuring the underlying resources from time to time as needed.

A server context that has visibility of the FP name space may directly configure the transport resources through the server context.

Components should SHOULD interact for specific management function, for example, such as connection management, route management, etc. The detail interaction description is described in clauses 8 and 11 of [ITU-T G.7702].

Client context SHALL support receiving and passing requests from administrator/client/higher level MCS to components which could deal with those requests. For example, CC establishes and releases connections on VNs within a client context.

Client context SHALL support requests of connection creation, deletion, modification with configurable parameters, such as SNP identifiers, direction of connection, connection constrains including capacity, layer, latency, cost, etc., required capacity.

9.3 Context interaction management

As described in clause 7.23 of [ITU-T G.7701], domains are established by operator policies. Example types of domains include management domain and control domain, which are referred in general as MC domain in this Recommendation.[ITU-T G.7718].

An MC domain may contain other MC domain(s) and thus in a hierarchical arrangement. In such case, the corresponding MCSs are hierarchically arranged.

The deployment of MCS in hierarchical levels and/or partitioned domains are based on the practical operational and administrative consideration of network management and control. When MC components interact across levels and/or domains, they need to interact through the interface (i.e., CPI) between contexts. This leads to the following consideration.

Clause 7.1 4 of [ITU-T G.7702] describes controller interaction where the requests to configure resources are passed, via a network call controller (NCC) from the server context of the client controller to the client context of the server controller. This leads to the following requirement on the server context NCC:

The server context NCC SHALL support resource configuration request via the CPI to the client context NCC of the server MCS.

Clause 7.25 of [ITU-T G.7702] describes that in the control of multi-layer network deployment, the client context of the server MCS manages the client layer network to the server layer network adaptation, and presents the resources to the server context of the client MCS as a client layer SNPP link, or as client layer subnetworks interconnected by SNPP links. The communication between contexts of MCS in adjacent levels is supported by a (multi-layer) NCC. This leads to the following requirements on the client context.

In controlling multi-layer network, the client context SHALL support control of the layer network adaptation and the client context NCC shall present the client layer SNPP link or client layer interconnected subnetworks via the CPI to the server NCC of the client MCS.

Client context ~~should~~SHOULD be capable to concatenate subnetwork and link connections through interface with NCC, which could supply ordered list of SNP pairs for requesting a connection.

When the connection status is affected by a defect in the transport resources that are in the scope of the MCS, the NCC of the client context in server MCS is responsible for sending the connection status update information to the NCCs of the server context in the client MCS.

Appendix I

Dispositioning/Mapping requirements

(This appendix does not form an integral part of this Recommendation.)

The following table is for dispositioning/mapping of the original requirements in the original and this edition of this Recommendation.

Req in v2.01	Clause in this version
R 1 A failure in the MP shall not affect the normal operation of a configured and operational CP or transport plane.	Clause 8.3
R 2 A failure in the CP-MP interface shall not affect configured services in the transport plane.	Clause 8.3
R 2.1 Upgrade of CP shall not affect configured services in the transport plane.	Clause 8.1
R 3 The MP shall not be affected (impacted) by a failure in the CP.	Clause 8.3
R 3.1 The failure and recovery of the CP-MP interface shall be detected by the MP.	Clause 8.3
R 3.2 The CP-MP interface shall support both centralized and distributed management of the ASON control plane.	Clause 8
R 3.3 The CP-MP interface information model shall be applicable for both centralized and distributed management of the ASON control plane.	Clause 8
R 4 The CP-MP interface shall support the assignment of identifiers for all identifier spaces, e.g., RA identifiers, SNPP identifiers, UNI/E-NNI transport resource identifiers, etc.	Clause 7.1.2
R 5 The CP-MP interface shall support the administration of identifiers including insuring their uniqueness within their respective spaces. In the case of protocol controller identifiers, this includes the relationship between the identifier and the point of attachment to the DCN.	Clause 7.1.2 and clause 8.2.1
R 6 It shall be possible to locate resources in one plane, i.e., the CP or the MP, and to navigate to the same resource from the other plane. General requirement of MC system.	Clause 7.1.2 and clause 7.2
R 7 The MP-CP interface shall support the ability to assign UNI/E-NNI transport resource identifiers per individual carrier's specifications.	Clause 7.1.2
R 8 The CP-MP interface shall support the ability to configure the binding, and retrieve the relationship, of a UNI/E-NNI transport resource identifier and the corresponding UNI/E-NNI SNPP identifier.	Clause 7.1.2 and clause 8.2.3
R 9 The CP-MP interface shall support the allocation of transport resources, e.g., CTPs, to the CP. Only one SNP in each SNPP can be associated with a CTP. Multiple SNPs (in different SNPPs) can be associated with a single CTP.	Clause 7.2
R 10 The CP-MP interface shall support the allocation of flexible adaptation resources to the CP.	Clause 7.2

Req in v2.01	Clause in this version
R 11 The CP-MP interface shall support the configuration of a specific SNP. The information to be configured for the SNPP members is: a) SNP/CTP relationship b) SNP parameters (SNP states as not validated, shared, etc.).	Clause 8.2.3 and clause 8.2.5
R 12 The CP-MP interface shall support the capability of assigning all CTP link connections in one trail to one SNPP link in one operation.	Clause 8.2.4
R 13 The CP-MP interface shall support the capability of binding SNPs to CTPs without having to manually provision each binding.	Clause 8.2.4
R 14 The CP-MP interface shall support the configuration of parameters required for diverse routing.	Clause 8.2.6
R 15 The CP-MP interface shall support for each SNPP, the configuration of the CP functions required to create/delete/modify the following interfaces: UNI, I-NNI and E-NNI.	Clause 8.2.1
R 16 The CP-MP interface shall support the transfer of routing database information between the MP and the CP.	Clause 8.2.6
R 17 The CP-MP interface shall support the ability to either assign or remove resources to/from the control plane. (When the transport resources are not being used to support any existing connections/connection segments, they can be moved from MP control to CP control or vice versa. Other scenarios, including the migration from MP to CP or vice versa, require further study.)	Clause 7.2
R 18 The CP-MP interface shall permit the MP to shut down specified transport resources. – See also [ITU-T X.731] for the definition of "shutting down" state.	Clause 7.2
R 19 The CP-MP interface shall support the ability to define one or more shared risk groups (SRG).	Clause 8.2.5
R 20 The CP-MP interface shall support the provisioning of a link to belong to multiple SRGs.	Clause 8.2.5
R 21 The CP-MP interface shall support the configuration of SNPP links which will include at least the provisioning of routing area information.	Clause 8.2.5
R 22 The CP-MP interface shall allow the configuration of the SNPP Link parameters needed for routing, signalling and management (name, directionality, cost, etc.).	Clause 8.2.5
R 23 The CP-MP interface shall allow single-ended SNPP link provisioning. Note that for this case, initial provisioning of the subnetwork names and SNPP name must be done at both ends.	Clause 8.2.5
R 24 The CP-MP interface shall permit the identity of CTP link connections to be provided to the CP by the MP.	Clause 7.1.2
R 25 The CP-MP interface shall support the configuration of the parameters necessary for UNI signalling, I-NNI signalling, and E-NNI signalling. A mechanism for detecting inconsistent settings for these parameters shall be provided.	Clause 8.2.1

Req in v2.01	Clause in this version
R 26 The CP-MP interface shall support the configuration of the parameters necessary for I-NNI routing and E-NNI routing. A mechanism for detecting inconsistent settings for these parameters, e.g., timers, shall be provided.	Clause 8.2.6
R 27 The CP-MP interface shall support the configuration of the parameters for individual ASON components. A mechanism for detecting inconsistent settings for the parameters shall be provided.	Clause 8.2
R 28 The CP-MP interface shall support the determination of a resource's assignment, i.e., assigned to the CP or the MP.	Clause 7.2
R 29 The CP-MP interface shall support the identification of inconsistencies between databases in the MP and CP.	Clause 8
R 29.1 CP-MP interface shall synchronize inconsistencies between databases in MP and CP.	Clause 8
R 30 The CP-MP interface shall support notifications of inconsistencies between the transport plane and the CP databases.	Clause 8
R 31 The CP-MP interface shall support the assignment of CP components to routing areas.	Clause 8.2.6
R 32 The CP-MP interface shall support the assignment of routing areas hierarchies.	Clause 8.2.6
R 33 The CP-MP interface shall support the assignment of CP components to hierarchical routing levels.	Clause 8.2.6
R 34 The CP-MP interface shall support routing area aggregation and disaggregation.	Clause 8.2.6
R 35 The CP-MP interface shall support reconfiguration of routing area hierarchies.	Clause 8.2.6
R 35.1 The CP-MP interface shall support the RC adjacencies configuration.	Clause 8.2.6
R 36 The CP-MP interface shall support the configuration of all the CP protocol controllers on a per interface or per group of interfaces basis. The specific protocol(s) selected for individual protocol controller shall be specified as follows: a) UNI signalling protocol; a.1) UNI discovery protocol; b) E-NNI signalling protocol; c) E-NNI routing protocol (if multiple protocols are supported); d) E-NNI discovery protocol; e) optionally I-NNI signalling protocol; f) optionally I-NNI routing protocol; g) optionally I-NNI discovery protocol.	Clause 8.2.1
R 37 The CP-MP interface shall support the assignment of the point of attachment to the DCN for each protocol controller. The MP must support the configuration of the binding of the control plane components (e.g., CC) to the protocol controller. Multiple protocol controllers may share the same point of attachment to the DCN. A network element may have multiple points of attachment to the DCN.	Clause 8.2.1

Req in v2.01	Clause in this version
R 38 The CP-MP interface shall support the configuration of each protocol controller. At a minimum, configuration of the following shall be supported: a) specific protocol for each controller among the protocols supported by a given system (specific protocol aspects are taken from the relevant protocol specifications); b) version number (if defined); c) protocol controller address.	Clause 8.2.1
R 39 Network elements supporting automatic discovery shall support a management information base for all discovered resources.	Clause 8.2.8
R 40 The CP-MP interface shall support notifications of the addition/removal/upgrade of CP objects.	Clause 8.1
R 41 The MP view of topology shall be independent of the CP protocol choice. – It should be noted that the format of the topology objects will be defined in Recommendations that address ASON information object specifications.	Clause 7.2
R 42 For intra-domain topology discovery, the CP-MP interface shall support notifications of the discovery of any changes to the intra-domain topology.	Clause 8.2.5
R 43 The CP-MP interface shall support notifications of the discovery of any changes to the inter-domain topology.	Clause 8.2.5
R 44 The CP-MP interface shall support the maintenance of hierarchical inter-domain topology information.	Clause 8.2.6
R 45 The CP-MP interface shall support the capability to query the CP for topological information.	Clause 8.2.6
R 46 The CP-MP interface shall support notification of failures in the link capability exchange procedure. The notification shall indicate the reason for the failure.	Clause 8.3.2
R 47 The CP-MP interface shall support notifications of a successful link capability exchange procedure. The notifications shall include service attributes for the UNI-C and UNI-N ports.	Clause 8.3.2
R 48 The CP-MP interface shall support the ability to manage calls with zero or more connections. For each call, the CP-MP interface shall support the ability to add, remove, or modify a connection.	Clause 8.2.2
R 48.1 The CP-MP interface shall support the ability to refresh the management plane and/or control plane view with changes that have occurred in the control plane as a result of call modification. This includes increasing/decreasing the bandwidth of an existing connection, increasing/decreasing the number of connections associated with the call, or increasing/decreasing the size of an inverse multiplexing group.	Clause 8.2.2
R 49 The CP-MP interface shall support the retrieval of call attributes including call name, calling/called UNI/E-NNI transport resource name, COS and GOS. The CP-MP interface shall also support the retrieval of call start and end times, and associated connections.	Clause 8.2.2

Req in v2.01	Clause in this version
R 50 The CP-MP interface must support the capability to distinguish an SPC from an SC. This is done via a call attribute that distinguishes the party responsible for end point handling of the call (i.e., whether the calling/called party call controller is at the UNI or the management plane).	Clause 8.2.2
R 51 The CP-MP interface shall support notifications from the CP of any defects associated with a call release request.	Clause 8.2.2
R 51.1 The CP-MP interface shall support call request success indication. The CP-MP interface shall support call request failure indications with a code identifying the reason for the failure.	Clause 8.2.2
R 52 The CP-MP interface shall support the capability to specify the explicit resource list for the management plane initiated connection set-up request. The explicit resource list is defined in clause 7.2.3.3 of [ITU-T G.7713].	Clause 8.2.7
R 53 The CP-MP interface shall support the ability to initiate CP directed maintenance rollovers.	Clause 8.2.7
R 54 The CP-MP interface shall support indications of a successful connection creation. The notification shall contain sufficient information to permit correlation with other connection segments.	Clause 8.2.7
R 55 The CP-MP interface shall support connection request failure indications with a code identifying the reason for the failure.	Clause 8.2.7
R 56 The CP-MP interface shall support indications of a successful connection re-route action.	Clause 8.2.7
R 57 The CP-MP interface shall support indication of the failure of a connection re-route action with a code identifying the reason for the failure.	Clause 8.2.7
R 58 The CP-MP interface shall support the retrieval of the status of all connections and the values of connection attributes.	Clause 8.2.7
R 59 The CP-MP interface shall support queries of all relevant attributes of CP controlled protected connections.	Clause 8.2.7
R 60 The CP-MP interface shall support the configuration of all relevant functions of CP controlled protected connections.	Clause 8.2.7
R 61 The CP-MP interface shall support the selection of the reversion process to be used with re-routed connections, e.g., manual or automatic reversion.	Clause 8.2.7

Req in v2.01	Clause in this version
R 62 The CP-MP interface shall support the ability to manage soft permanent connections, including those that make use of VCAT and LCAS functions. Specifically, the following shall be supported: a) The ability to invoke the set-up of a soft permanent connection. b) The ability to invoke the release of a soft permanent connection. c) The ability to invoke the modify operation of a soft permanent connection. d) The ability to invoke the re-routing of a soft permanent connection. e) The ability to query the CP for the status of a soft permanent connection. f) The ability to query the CP for the connection attributes of a soft permanent connection including route information. g) The ability to allow the MP to request a VCAT SPC with different service levels (making use of diverse routing of bundles). h) The ability to allow the MP to modify SPCs which make use of the VCAT and LCAS functions, i.e., to increase or decrease the bandwidth without service interruption. i) The ability to support the provisioning of class of service parameters, which may be mapped to protection/restoration mechanisms and configurations within the networks.	Clause 8.2.7
R 62.1 The CP-MP interface shall support requests for migration from a PC to a SPC. The transport resource supporting the PC should be moved from the scope of the MP to the scope of CP without service disruption. A call with the appropriate parameters (including state information) shall be created such that the CP can manage the call.	Clause 8.2.7
R 63 The CP-MP interface shall support the ability to specify an SPC using class of service parameters which may be mapped to constraint-based routing. This may include, but are not limited to link, node and SRG diversity.	Clause 8.2.7
R 64 The CP-MP interface shall support requests for switched connections (SC). This support shall include: a) Notifications of the set-up, release, and modification of SCs. b) The ability to invoke the release of an SC. c) The ability to invoke the re-routing of an SC. d) The ability to query the CP for the status of an SC. e) The ability to query the CP for the connection attributes of an SC including route information. f) The ability to support the provisioning of class of service parameters, which may be mapped to protection/restoration mechanisms and configurations within the networks.	Clause 8.2.7
R 65 The CP-MP interface shall support the exchange of information pertaining to switched connections created in the network. NOTE – [ITU-T G.7713] and the ITU-T G.7713.x-series of Recommendations contain specific information on connection attributes.	Clause 8.2.7
R 66 The CP-MP interface shall support the configuration of policy parameters.	Clause 8.2.1

Req in v2.01	Clause in this version
R 67 The CP-MP interface shall support querying of policy parameters.	Clause 8.2.1
R 68 The CP-MP interface shall support the configuration of CP alarm characteristics.	Clause 8.3
R 69 The CP-MP interface shall support autonomous alarm notification from the CP for each CP fault. Information in the notification shall include the resource in alarm, the time the alarm occurred, the probable cause, and the perceived severity of the alarm.	Clause 8.3
R 70 The CP-MP interface shall support the ability to query all or a subset of the currently active CP alarms.	Clause 8.3
R 71 The MP shall administer the CP alarm severity in accordance with the TMN requirements specified in [ITU-T M.3100] and [ITU-T M.3120].	Clause 8.3
R 72 The CP-MP interface shall support querying of the operational state of CP components.	Clause 8.3
R 73 The CP-MP interface shall support the collection of the necessary current and historic usage data, such as call attempts, call set-up failures including reasons and successes. The data should be available upon the query from the management plane.	Clause 8.4
R 74 The CP-MP interface shall support queries of the connection attempts, connection set-up failures and successes.	Clause 8.4.2
R 75 The CP-MP interface shall support the ability to query current and historic CP performance data. Specific performance parameters for the CP are for further study. A possible parameter is the number of connection re-routing events per call.	Clause 8.4
R 76 The CP-MP interface shall support the ability to retrieve SNPP link usage information from the CP.	Clause 8.4.1
R 77 The CP-MP interface shall support per UNI and E-NNI an appropriate notification of failed connection set-ups, failed connection re-routes, etc., that exceed a configured threshold.	Clause 8.4
R 78 The CP-MP interface shall support the capability of querying CP for a batch of call detail records.	Clause 8.5
R 78.1 Call details record shall be available after a call terminated.	Clause 8.5
R 78.2 Call details record shall include attributes such as customer identification, call start time, call end time, bandwidth, grade of service, and call type (i.e., SPC or SC).	Clause 8.5
R 79 The CP-MP interface shall support notifications of a CP restoration failure.	Clause 8.2.7
R 80 The CP-MP interface shall support the provisioning of timers (e.g., revert and restore) per re-routing domain.	Clause 8.2.7

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	**Y.1700–Y.1799**
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
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, and associated measurements and tests
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, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023