ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T G.7716/Y.1707 (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

---

Architecture of management and control operations

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.7716/Y.1707

Architecture of management and control operations

Summary

Recommendation ITU-T G.7716/Y.1707 addresses the architecture of management and control operations. This Recommendation provides guidance for service providers on the transport network plan, initialization, performing typical operations and maintenance in the network.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.7716/Y.1707	2010-01-13	15	11.1002/1000/10421
2.0	ITU-T G.7716/Y.1707	2022-11-13	15	11.1002/1000/15145

Keywords

Architecture, control, management, operation.

* 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.7716/Y.1707

Architecture of control plane operations

1 Scope

This Recommendation provides guidance for service providers on:

– how to plan a transport network with management-control (MC) systems;

– how to initialize the transport network with MC systems;

– how to operate and maintain the transport network with MC systems.

This Recommendation also provides guidance to MC function and protocol designers on the sort of operations MC protocols and implementations they need to be able to support.

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

[ITU-T G.7702] Recommendation ITU-T G.7702 (2022), *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), *Common equipment management function requirements*.

[ITU-T G.7712] Recommendation ITU-T G.7712/Y.1703 (2008), *Architecture and specification of data communication network.*

[ITU-T G.7714] Recommendation ITU-T G.7714/Y.1705 (2005), *Generalized automatic discovery for transport entities*.

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

[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.7718] Recommendation ITU-T G.7718/Y.1709 (2020), *Framework for the management of management-control components and functions*.

[ITU-T G.7719] Recommendation ITU-T G.7719 (2021), *Management information model for management-control components and functions*.

[ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 platform [b-ITU-T X.638]: An implementation of an identified platform specification.

3.1.2 platform specification [b-ITU-T X.638]: The functional specification of a formal programmatic interface and a set of supporting local services for an identified stack specification.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 commissioning: The act of specifying parameters necessary to create a control domain instance.

3.2.2 provisioning: The act of specifying the parameters necessary when assigning/deassigning network resources to/from the control domain or to invoke/remove services provided by a control domain instance.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AN	Abstract Node
ASON	Automatically Switched Optical Network
BN	Boundary Node
CC	Connection Controller
CD	Control Domain
CCN	Control Communication Network
DA	Discovery Agent
DCN	Data Communication Network
E-NNI	External Network-Network Interface
FCAPS	Fault management, Configuration management, Accounting management, Performance management, Security management
FP	Forwarding Point
ID	Identifier
I-NNI	Internal Network-Network Interface
LRM	Link Resource Manager
MCS	Management Control System
NCC	Network Call Controller
NE	Network Equipment
OSPF-TE	Open Shortest Path First – Traffic Engineering
PC	Protocol Controller
RA	Routing Area
RC	Routing Controller

RSVP-TE Resource reservation Protocol – Traffic Engineering

SCN Signalling Communication Network

SDN Software Defined Networking

SN Subnetwork

SNP Subnetwork Point

SNPP Subnetwork Point Pool

SLA Service Level Agreement

TAP Termination and Adaptation Performer

TMN Telecommunication Management Network

TRI Transport Resource Identifier

UNI User Network Interface

VN Virtual Network

VPN Virtual Private Network

5 Conventions

None.

6 Overview of MC deployment

The design of a transport network requires network planning as well as traffic planning. The process of network planning determines the network design given a traffic forecast. Network planning processes could apply to only parts of a network, e.g., subnetworks (SNs). The process of traffic planning determines the way that traffic predicted in the traffic forecast will be routed using existing network resources. The process of capacity install is based on the service request from the customer, and activates the network resource for the assigned traffic.

These two processes are constantly attempting to provide the highest quality service at the least cost to the operator. They separately exist as they operate in two different time scales – the process of building new network resources (i.e., fibre routes, central offices, network equipment (NE) deployment) to deal with new traffic predicted in a network forecast takes months to years while the process of establishing trunks using existing resources may take only minutes to weeks.

Traffic forecasts are periodically developed based on trends, advance information from customers and macro-economic factors. Since these inputs are dynamic, the forecast is also dynamic.

Figure 6-1 shows the three processes in transport network design and operation phases. The result of the traffic planning process is the input to the network planning process, and the network resource is activated by the capacity install process.

Software defined networking (SDN) technology can also provide the functionalities on traffic planning and network planning. The local capacity and traffic demand can be reported from the network to the controller and be optimized in a more dynamic way. After deployment, both the controller and the equipment will need to update the database to sync up with the upgraded network, including the automatically switched optical network (ASON) characteristic sync up for old equipment and SDN controller, and the capability installation on new equipment.

SDN technology and ASON are complementary and interwork with each other in the network. Common aspects are described in [ITU-T G.7701], by taking the mixed architectural approaches into account.

Before the network planning process starts, the operator should collect the traffic demands. These demands may come at different times. The network planning process can be started when one demand comes and reiterated when there are other demands. So the demands are grouped, and the network planning process is periodically executed.

The network initialization is divided into physical and virtual parts. For the physical part it is mainly the capacity install, while for the virtual part it is mainly the set-up of the MC systems to run various of configuration through different protocols.

The network operation and maintenance start after the network is initialized. MC systems are collaborating with each other to guarantee the network running without any problems. Performance on the network is consecutively monitored by the operator to capture the status of the network, and recovery/reconfigurations are needed once there are special events such as faults and alarms.

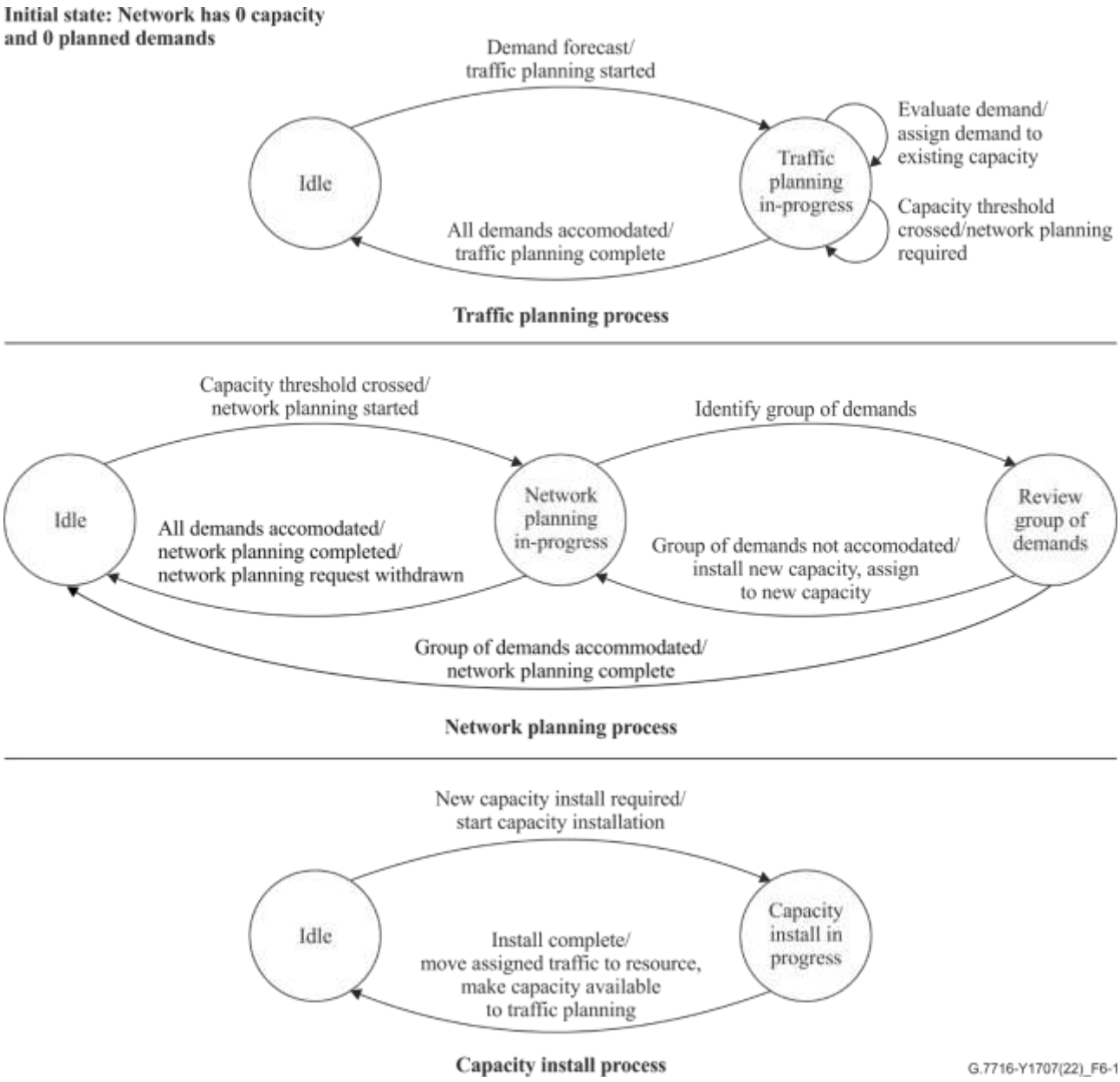

Figure 6-1 – Three processes in transport network design and operation phases

7 Transport network planning

As a part of the network engineering process, a transport network planning is developed and refined. This planning specifies the fundamental information needed to set up and operate a transport network controlled by a management control system (MCS). Based on [ITU-T G.7701], the MCS instance could be ASON control, SDN controller, NMS and any combinations among them. The information in the transport network plan can be divided into three categories: Transport network resource, MCS infrastructure and control communication network (CCN) infrastructure. It is worth noting that the transport network resource can be either physical and/or virtual from the perspective of MCS, and the planning described in this clause should be applicable to both physical and virtual transport network resources. Detailed characteristics for virtual transport network resource planning are described in clause 10.

When there are multiple MC systems in the network, the network planning is conducted in a joint manner. A global view of the network is needed to be collected to one MC system to plan the network. One of these systems would be designated as the leading system before the planning starts. Other systems are considered as the supporting systems which provides the detailed data to the leading system. Stitching would be needed, in the leading system, in order to form the global view.

7.1 Transport resource planning

The transport network resource planning includes the following information:

- subnetwork/routing area definition (Note 1);
- layer network relationships;
- subnetwork/routing area hierarchy;
- topology abstraction;
- addressing structure (Note 2).

NOTE 1 – Subnetworks and routing areas are functionally identical, with some subtle differences. Clause 6.2 of [ITU-T G.7703] describes these differences.

NOTE 2 – These addresses are for the transport resources and should not be confused with addresses in use in a CCN for ASON.

Due to the dynamic nature of traffic forecasts, the transport network plan needs to be flexible – it must accommodate changes in network engineering, under the coordination from multiple control systems. These may be manifested in changes to the data plane topology as well as to the signalling network, component adjacencies and even functional component distributions. The representation of such changes in ASON control domain and SDN controllers should be correct and consistent.

7.2 MC System infrastructure

MC function (in MC components) may be contained in MC systems of which three types are shown: SDN, ASON and others. Each instance of an MC system has in its scope a set of transport resources over which it supports connection management in a layer network. The common control components for SDN and ASON are specified in [ITU-T G.7701]. The management functions would include the instantiation of an MC system and its components, assignment of transport resources to the scope of an MC system, etc. Management functions recur and a management function instance can manage a set of other management function instances. The management requirements of the MC components and functions are specified in [ITU-T G.7718]. [ITU-T G.7719] provides a protocol-neutral management information model for MC components and functions. The protocol-neutral management information model should be used as the base for defining protocol-specific management information models. This Recommendation uses the ITU-T G.7719 information model when describing operational procedures. How implementations provide the information model and any operations necessary to synchronize the internal operation of the model implementation are out of scope of this Recommendation.

Transport resource management functional areas are identified in [ITU-T M.3010] as: performance management, fault management, configuration management, accounting management and security management. These management functions could be contained in another MC system which could be instantiated as an OSS/NMS/EMS.

For ASON, the network planning information includes:

- protocol selection;
- control component distribution;
- signalling network design;
- control component adjacency design.

For SDN, the network planning information includes:

- network topology design;
- status check for nodes/links;
- connectivity design;
- data communication design;
- control components installation.

Due to the dynamic nature of traffic forecasts, the transport network plan needs to be flexible – it must accommodate changes in network engineering, and the changes may be decided under the coordination of multiple control systems. These may be manifested in changes to the transport network topology as well as to CCN, component adjacencies and even functional component distributions. The representation of such changes in ASON control domain and SDN controllers should be correct and consistent.

7.3 CCN infrastructure

[ITU-T G.7712] defines the architecture requirements for a DCN which may support, among other applications, the distributed management communications related to the telecommunication management network (TMN), distributed signalling communications related to the ASON, distributed control communication related to the SDN and other distributed communications. This Recommendation uses the [ITU-T G.7712] architecture to describe the CCN available to control domains and notes that the control components may be dependent on that CCN infrastructure. Configuring and managing the CCN infrastructure is outside the scope of this Recommendation.

8 Transport network initialization

Initialization is the process of determining what resources exist, that they need to be bound to the appropriate MC functional components, and that the MC functional components need to array themselves into the appropriate confederation. This clause recognizes that certain information needed to accomplish this must be provisioned by the network administrator.

Besides physical resources, a multi-domain or multi-layer network is usually composed by multiple MC systems. The responsibility of initialization in these networks can be decomposed into multiple single-domain or single-layer network. Based on the decomposition, many smaller networks with single MC systems can be initialized respectively.

One leading system would be needed to collect the status of the initialization for each piece in the network. Every other system can be considered as supporting systems to provide the feedback to the leading system once the initialization is done. The leading system will know that the initialization has been completed once every supporting system has completed their own initialization.

8.1 Commissioning

Commissioning is the process of initial configuration used to provide a network element with critical binding information, network-wide naming information and global protocol parameters. These parameters are fundamental to the continued operation of the control domain instance and cannot be changed without significant impact to the control domain instance. Therefore, commissioning is only done during the initialization phase of the control domain lifecycle. Note that commissioning is focused on the commissioning on the control domain component and not the transport resource. Functional components are bound via operations on the management information, introduced in clause 8.1.2 and specified in [ITU-T G.7718].

The information provided to the network element in the commissioning phase consists of the critical parameters identified as a part of network planning. The commissioning phase of a network element could be done automatically by the NE with minimal manual intervention. For example, DHCP could be used by the NE to get appropriate IP address configurations. Other critical parameters for commissioning could be passed to the NE after the communication channel has been set up.

Some configurations must be completed such as the node ID, area hierarchy, and so on, before the control domain starts up through initialization. The procedures of the local initialization include two steps: MC component activation and MC component binding. As initialization is performed, the components shall report transitions in status to the element management function [ITU-T G.7710].

8.1.1 MC component activation

The tasks and processes that support the functions described by the MC components are activated through object creation operations on the management information model. For example, a routing protocol controller is instantiated by creating a routing protocol object. Internal operations within the network element to carry out activation are outside the scope of this Recommendation.

The order of managed object creation must take into account the dependencies that exist between the objects. For example, routing areas must be created first, as subnetwork point pool (SNPP) names include the routing area identifier. Likewise, an adjacency between distributed signalling protocol controllers may depend on the configuration of a link for which it is responsible, and so cannot be created before the link has been created.

8.1.2 MC component binding configuration

The MC components local to a MCS or on peer MCSs must coordinate with each other to fulfil the management and control domain functionality, so these MC components must be associated with each other in either a physical or a logical way. This Recommendation discusses the binding required between MCSs supporting MC functions. The bindings internal to an MCS are a matter of the implementation and are outside the scope of this Recommendation.

The relationship between MC components is illustrated in Figure 6-1 of [ITU-T G.7701]. The bindings of the components need to be established at the initialization stage. These bindings may be software bindings or remote interface bindings, either physical or virtual. They may be static, provisioned or dynamic. Examples of bindings are NCC-CC, CC-RC, RC-LRM, as well as inter-level MC system interaction, etc.

An SNPP is controlled by a specific connection controller (CC), routing controller (RC) and link resource manager (LRM) component. These components must be bound to each other in order to perform the control function. The bindings between CC and RC, RC and LRM as well as CC and LRM may be established before SNPP links have been created between routing areas.

8.1.3 Routing initialization

The prerequisite information for routing object activation includes routing operational style (i.e., centralized/distributed path computation) as this controls routing protocol neighbour adjacencies, addressing (including routing area hierarchy and subnetwork identifiers). The

operational style is predefined by the operator and the other information could be embedded in the equipment by the manufacturer or could be accessed from a configuration store when the equipment is installed. In the context of virtual network (VNs), all the adjacency and identifiers are logical and have a local mapping to physical equipment, and the routing initialization can be done based on this logical information.

The association between routing areas (RAs) (e.g., child RA and parent RA, local RA and remote RA, physical RA and virtual RA) is configured by providing the correct identifiers in the created Routing Area objects.

In order to support the establishment or maintenance of network connections and available network topology, each routing table object should have consistent topology information about the network.

The adjacencies between RC PCs within a routing area must be established to support the advertising and maintenance of the available SNPP link topology. Virtualization can be applicable between RCs to instantiate the SNPP link from one RC to another. The information of the peer RC PCs (such as signalling communication network (SCN) address) can be manually configured or dynamically discovered during the adjacencies set-up process.

In the case of hierarchical routing, adjacencies between lower level RCs and upper level RCs in the corresponding parent routing area are established when the "parent routing area" and "child routing area" parameters are configured on the "routing area" object. This supports the hierarchical routing information collection, maintenance and the hierarchical routing computation. The information of the hierarchical RAs is configured or dynamically discovered during the adjacencies set-up process.

Note that hierarchical routing may result in multi-RCs and multi-PCs. In this situation, the relationship between those RCs and PCs should be properly maintained during routing initialization.

RC PCs are configured when a routing protocol is selected for an adjacency during routing initialization. Per [ITU-T G.7703], the type of routing approach (i.e., step-by-step, source routed, hierarchical) is not restricted. The protocol selected will determine the specific configuration information that is required to initialize the RC PC. This protocol-specific configuration is given as a part of the RC PC creation. [ITU-T G.7719] provides the specific attribute information required when creating an RC PC managed entity.

Per [ITU-T G.7703] and [ITU-T G.7715], there may be several protocol controllers supported for routing information exchange. The routing architecture allows for support of multiple routing protocols. This is achieved by creating different routing protocol objects, which may result in several protocol controllers being instantiated. The architecture does not assume a one-to-one correspondence between routing controller instances and protocol controller instances. During the routing initialization procedure, the relationship between PCs and RCs should be properly configured.

A virtual private network (VPN) is a construct within a single layer network and can be created by:

1) explicitly allocating network resources for it;

2) sharing common network resources among multiple VPNs.

VN is a more generic term that can not only be used in single layer network but also multi-layer network. Besides the characteristics in VPN, the VN can also be created by combining network resources from multi-layer networks.

8.2 Reconfiguration during commissioning for MC component

During the commissioning state, reconfiguration of commissioning parameters may be performed without impact. This is different than reconfiguration while in the operations and maintenance state as the impact to active services provided by the MC is different. During the commissioning state, the MC components have not been placed into service yet. As a result, changes in the configuration of

critical MC components will not impact the set-up of new calls and connections or the continuation of existing calls and connections.

Some configurations during commissioning may have been done for trialling purposes, so the operator needs to reconfigure some information according to the practical network environments for the MC functions. For example, ASON control domain security functions should be tested, so encrypting open shortest path first – traffic engineering (OSPF-TE) or resource reservation protocol – traffic engineering (RSVP-TE) may be configured to examine the validity. However, according to current practical network environments, there is no need for control domain security, so the configuration should be reconfigured.

Most configurations during commissioning may be configured by a manual process which would be prone to manual errors, so the reconfiguration should also be initiated in the case of a manual mistake. For example, the configured node IDs for some nodes may conflict, so these node IDs need to be reconfigured. For another example, the binding relationships between MC components described in clause 8.1.2 may be configured by mistake, so these binding relationships should also be reconfigured.

Incorrect configuration during the commissioning state should be detected by MC components and reported to the MC. This notification would allow an operator to correct these errors before progressing to the operations and maintenance state.

9 Transport network operation and maintenance

The operation and maintenance for a multi-domain or a multi-layer network is basically repeating the single-domain/layer operation and maintenance with coordination. From the perspective of one operation and/or maintenance functionality, such coordination includes synchronization among systems and workload sharing. One leading system is needed to distribute the workload to multiple supporting systems in the network, to conduct the operation and maintenance. The status of the work are reported to the leading system and the workload may be reallocated for balancing between supporting MC systems.

9.1 Provisioning

Provisioning is the process of incremental configuration performed when service instances are configured on or resource changes are made to a network. The parameters specified by provisioning are specific to a resource or service request, and making changes to those parameters will only affect the specific resource or service request. Provisioning is allowed in the initialization and operations phases of the control domain lifecycle. Resource changes may be the result of assigning an SNPP link to or removing an SNPP link from the control domain, or the modification of an SNPP link property. Modifications made to SNPP link properties include the binding of additional SNP link connections into an SNPP link or the binding of a transport resource identifier (TRI) to an SNPP.

When a link has link connections being used by a call in a network, the link should not be deleted before the services are successfully removed. Note that property modifications to a link that bears services must be made carefully because although some properties of the link may be modified (e.g., the protection capability advertised for a link), some other properties must not be modified (e.g., reducing the link protection provided by the transport resource below the protection level being advertised).

The MC has a full view of the properties of the link, and the control domain only has a partial view of the properties of the link, which may be advertised by routing protocols.

Provisioning can be performed by the MC. When a configurable item is provided by the MC, it has higher standing than a configuration determined by the discovery agent. When a mismatch occurs between configuration provided by the MC and configuration determined by the discovery agent, the MC configuration shall be maintained, and an alarm shall be raised to allow the management system rectify the mismatch.

Provisioning is the process of creation, trivial reconfiguration and destruction of an entity in the system, such as discovering/configuring and releasing/deleting a link of the network.

9.2 Resource assignment

A transport resource can be allocated by the MCS to any specific network or VN according to the demand. Such kind of allocation can be driven either by operators or by customer requirement. For example, resources with one same switching technology can be allocated to the same layer, while the resources delivered to the same services are requesting specific service level agreements (SLAs).

A transport resource can be assigned to one or more VNs. When the resource is assigned to only one VN, it is dedicated to that VN. When the resource is assigned to more VNs, it is shared between the VNs, and the resource assignment states should also be consistent among them.

The administrator of an MC system can create a client context and assign some resources for it based on the VN requirements or constraints from client controllers or external applications. In the client context, the assigned resources can be virtualized into VNs for client controllers or external applications.

The creation and deletion of control artefacts are defined in [ITU-T G.7719].

The MCS is responsible for maintaining the persistent store of configuration information.

9.3 Discovery/authentication process

The result of the discovery/authentication process can be utilized by the control domain for the link configuration process. The high-level process for accomplishing this is described in [ITU-T G.7714]. The mapping between the physical and virtual link needs to be maintained by MCS, and the interfacing referring to the specific network resource should be using consistent name space for mutual understanding, to guarantee the correctness of discovery and authentication.

As the discovery process is performed, the information discovered should be validated by the control domain instance against the existing configuration. This validation is discussed as part of auditing.

9.3.1 Neighbour discovery

The neighbour discovery process identifies the existence of a neighbour binding to a local resource.

By operating the neighbour discovery process and link discovery process, information related to the link resources and the remote end of the link connections can be obtained. This information may be used either to configure the local MC components or to verify the parameters configured by the MC.

As part of the link establishment process, the state of any transport resource adjacencies which are dynamically discovered should be verified with the service provider's policy before those resources are added to SNPP links.

A neighbour relationship needs to be established between MC components in different level controllers and transport elements to start the subsequent network resource management process. There are two solutions to this problem. The first is to configure the neighbour relationship between upper MC components and lower MC components based on network planning and design. The second is to set the upper MCS as the service party, automatically allocate the network address for the lower network MC component, automatically establish the neighbour relationship, and realize the plug and play function for network equipment.

9.3.2 Link discovery

The link discovery process identifies the link attributes which are configured at both endpoints of the link connection by the MC. The link attributes may include the local SNPP link ID, remote SNPP link ID, signal type, link weight, resource class, local connection types, link capacity, link availability, diverse support, local adaptation support and reachability information.

For inter domain link discovery under MCS architecture, the SNP of inter-domain links need to be identified to distinguish them from those of intra-domain links. This inter-domain link ID can be configured by the domain MCS through network planning and design, and then reported to the inter domain MCS.

− Intra domain link discovery:

In the SDN MC system, intra domain link discovery can be completed through link discovery protocols such as LLDP.

In ASON MC system, intra domain link discovery for controlling usage is usually completed by dynamic protocols such as LMP and OSPF.

− Inter domain link discovery:

Inter domain link discovery could be done automatically or manually according to the specific domain deployment and scenario. When the automatic discovery method is adopted, the adjacent domains need to negotiate the interaction identification in advance. Then, the inter domain link discovery is carried out by the combination of single domain link discovery method and domain identifications. While the manual method is adopted, the inter domain link would be set by administrators through MC system(s).

9.3.3 Management and control capability discovery

The management and control capability discovery process identifies the management and control capability supported by MC system and network element. The management and control capability may include the version information of the protocols, the supported information models and supported operations over it.

9.4 Link configuration

The underlying resources being used by a link should be tested and deemed fit for use prior to the link configuration process.

Link configuration can be established by manual configuration or dynamic discovery. The dynamic discovery mechanism may be performed by exchanging some extra identifier information during the transport entity capability exchange.

9.4.1 Overview

Configuration of a new link in the control domain requires a number of items, including SNPP names, routing controller PC SCN address, etc. However, before these items can be identified, the trail must be located in the overall network topology. Therefore, the routing area for the link must be identified and the SNPP names for the link ends determined before any other link configuration can be completed.

Once naming has been established, the configuration information necessary for signalling adjacency (i.e., connection controller and call controller) and routing adjacency establishment is configured. This information includes the signalling controller adjacency configuration information (CC ID, and CC PC SCN address), and (if appropriate) the network call controller adjacency configuration information (NCC ID and NCC PC SCN address) as well as the routing adjacency configuration information (RC ID and RC PC SCN address).

This clause does not discuss the MC configuration performed for adding a link.

9.4.2 Authorization

Before adding a link to the control domain, the identity of the node at the other end of the link is determined and authorized. This identity information in turn is used to drive policy that determines what sort of interactions will be allowed with the far node. The policy may control things such as whether the transport resource is associated with a user network interface (UNI) or an E-NNI reference point, the type of services that may be requested, etc.

9.4.3 Link naming

A naming exchange is done to identify the routing area for the link and the SNPP names for the link ends before any other link configuration can be completed.

An SNPP name consists of either one or more nested RA names, an optional subnetwork (SN) name and link context (LinkContext) names. An SNPP alias is an alternate SNPP name for the same SNPP that may be generated from another SNPP name space.

Within a layer network fragment, the routing area for the link is the lowest area (i.e., furthest from the network root) that is common for both ends of the link. To identify this, the routing subsystem requires having an ordered list of areas, starting with the root of the routing hierarchy, for both ends of the link.

This information is passed in the naming exchange phase of the transport entity capability exchange. Once provided with this information, as well as the local end's SNPP name in the lowest area in the list, the control domain can determine the SNPP alias and routing area ID for the local link end, and exchange it with the remote end. This information is then provided to the link resource manager (LRM).

Figure 9-1 shows the SNPP name of the end of Link_1 in level 0, and the end of Link_1 in level 1.

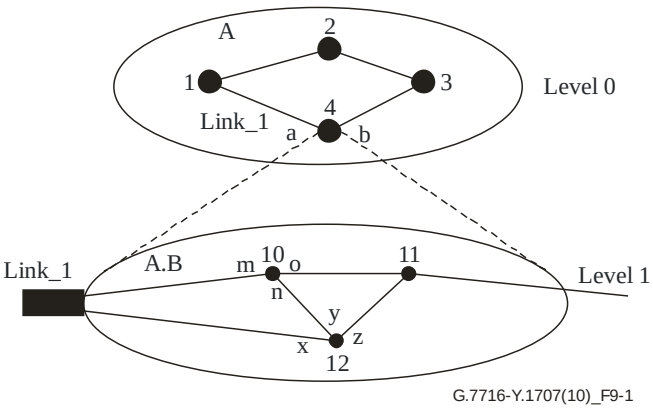

Figure 9-1 – Example of SNPP alias use with abstract node

The SNPP name of the end of Link_1 in level 0 is {A.4.a}, where "A" is the routing area ID in level 0, "4" is the subnetwork name, and "a" is the link context name.

The SNPP name of the end of Link_1 in level 1 is {A.B.10.m, A.B.12.x}, where "A.B" is the routing area ID, "10" and "12" are the subnetwork names, and "m" and "x" are the link context names.

So the SNPP name of the end of Link_1 in level 1 is the SNPP alias of the end of Link_1 in level 0, and the SNPP name {A.4.a} is equal to the SNPP name {A.B.10.m, A.B.12.x}.

Figure 9-2 shows the SNPP alias used with abstract topology. The SNPP name of the end of Link_1 in level 0 is {A.4.a, A.5.e}, where "A" is the routing area ID, "4" and "5" are the subnetwork names, and "a" and "e" are the link context names.

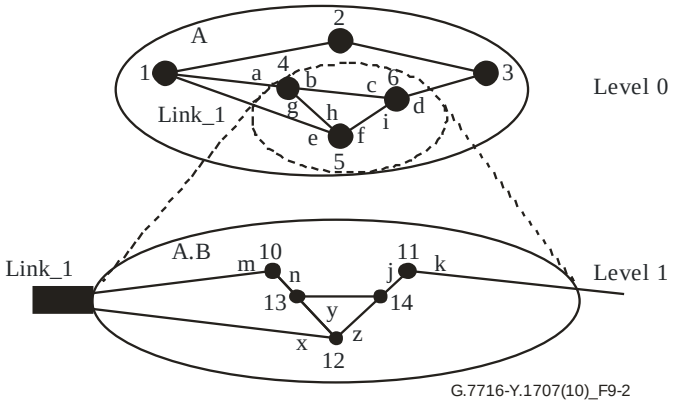

Figure 9-2 – Example of SNPP alias use with abstract topology

The SNPP name of the end of Link_1 in level 1 is {A.B.10.m, A.B.12.x}, where "A.B" is the routing area ID, "10" and "12" are the subnetwork names, and "m" and "x" are the link context names.

So, the SNPP name of the end of Link_1 in level 1 is the SNPP alias of the end of Link_1 in level 0, and the SNPP name {A.4.a, A.5.e} is equivalent to the SNPP name {A.B.10.m, A.B.12.x}.

9.4.3.1 Use of alternate SNPP names for flexible adaptation

See clause 6.3 of [ITU-T G.7703] (topology and discovery).

9.4.3.2 Use of alternate SNPP names for VPNs

See clause 6.3 of [ITU-T G.7703] (topology and discovery).

9.4.3.3 Use of SNPP aliases for routing hierarchy

The use of SNPP aliases for routing hierarchy is described in Appendix I of [ITU-T G.7715.1]. When SNPP aliases are used this way, each routing hierarchy level may use SNPP names from area-specific SNPP name spaces to reference a link resource. Establishing the equivalence of these names is performed at the time the link is established. The name space mapping may be stored in a directory service component to facilitate establishing the equivalence.

9.4.4 Signalling initialization

In order to support the establishment or maintenance of call and network connection, the signalling adjacencies need to be established between the peer control components.

The adjacencies between all CCs and the corresponding peer CCs need to be established to support the establishment and maintenance of the network connection. The information of the peer CCs (such as CC ID, CC PC SCN address) can be manually configured or dynamically discovered during the adjacencies set-up process.

In order to support the call process, the adjacencies between CCC and NCC as well as between NCCs also need to be established. The information used to establish these adjacencies (such as CCC/NCC ID, CCC/NCC PC SCN address) can be manually configured or dynamically discovered during the adjacencies set-up process.

When a joint federation model is used by connection management in the inter-domain context, the adjacencies between related CCs need to be established. The information used to establish the CC adjacencies (such as CC ID, CC PC SCN address) can be manually configured or dynamically discovered during the adjacencies set-up process.

9.4.5 Routing initialization

Routing adjacency may need to be created to connect the routing controller associated with the end point of a transport link to other routing controllers within the routing area. See clause 9.5 for the specifics of routing adjacency configuration.

9.5 Routing adjacency configuration

Three types of routing message distribution topology are described in [ITU-T G.7715], which illustrates how to locate the routing adjacency:

– for a congruent topology, the routing adjacency is congruent with the transport network;

– for a hubbed topology using a routing message server, the routing adjacency of each routing controller is the message server;

– for a directed topology, the routing adjacency topology is determined by the network administrator.

For a congruent topology, routing adjacencies may be established as a part of configuring SNPP links. For hubbed and directed topologies, the routing adjacencies are provisioned as a separate action from link configuration. This allows the adjacencies to be established prior to link configuration.

The routing adjacency is configured by sharing the local RC ID and RC PC SCN address with the peer of the adjacency. This means that the remote end will provide its RC ID and RC PC SCN address to the local end. In the centralized and hierarchical routing architecture, besides the neighbour configuration in the physical layer, it is also necessary to configure the adjacency between the lower-level RC and the upper-level RC, or the neighbour relationship between the gateway RC and the upper-level RC. When the upper-level RCs are deployed with protection, there is also the primary (active)-secondary (standby) relationship, the lower-level RC shall configure the neighbour relationship with the upper-level primary and secondary RC at the same time.

The upper-level RC and the lower-level RC can form a neighbour relationship through sharing the local RC ID and RC PC SCN address.

9.6 Reconfiguration

Reconfiguration during the operations and maintenance state requires critical MC components being taken out of service. This will impact the control domain's ability to set up new calls and connections as well as maintain existing calls and connections. As a result, reconfiguration requires a strategy to reduce the impact on the users of the control domain. The strategy required is specific to the type of reconfiguration being performed and the MC components it affects.

9.6.1 Strategy for SNPPID changes

One or more than one SNPPIDs can mapped into one transport resource identifier. When there is a change in routing area ID, the corresponding SNPPIDs will be changed. To facilitate the change of routing area ID, SNPP aliases will need to be established as described in clause 9.4.3. Once established, affected connection and call records need to be updated to reflect the new SNPP alias after which the old SNPPID can be gracefully withdrawn.

9.6.2 Strategy for routing area changes

In the process of operating networks, reconfigurations will be performed on a physical or virtual routing area. The reasons for reconfiguration of a routing area may be administrative or business activities. For the administrative motive, in some cases, if there are so many nodes in a routing area that it is not easy to manage the network, it requires that the routing area should be split into several smaller routing areas or virtualize it via abstracting some nodes. For business activities such as acquisition/merger or divestiture, when these transactions take place, it will result in routing area merging or deletion.

There are four typical reconfigurations performed on a routing area:

– Splitting one RA into two or more separate RAs.

– Merging two or more RAs into one RA.

– Creation of an RA into the hierarchy.

– Deletion of an RA from the hierarchy.

It is worth noting that reconfiguration is also applicable in VNs and is usually more frequently used if compared with physical networks. As these reconfigurations radically impact routing, they should be planned carefully in order to reduce the impact of routing oscillation on the service. These reconfigurations should be performed during low traffic, such as at midnight. If the reconfiguration impacts the policy boundary, then signalling and traffic are also impacted.

9.6.2.1 Routing area splitting/merging

When the merge of two routing areas or the split of a routing area into two routing areas is performed, the routing structure should be reconfigured. In order to reduce the routing oscillation, the routing hierarchy should be maintained steadily as possible as before.

The general procedures of routing area splitting and merging are described below.

9.6.2.1.1 Routing area splitting

The following example shows the procedures of a single hierarchical level routing area splitting.

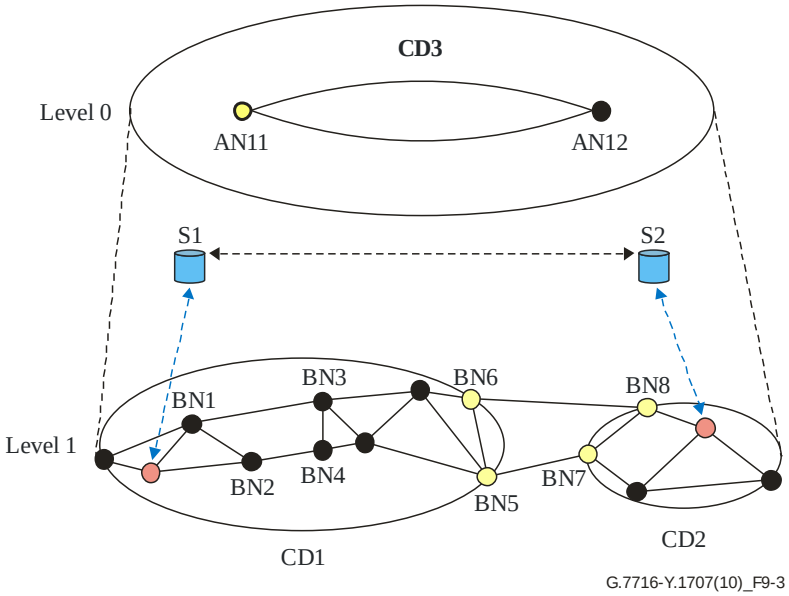

Figure 9-3 – Initial topology

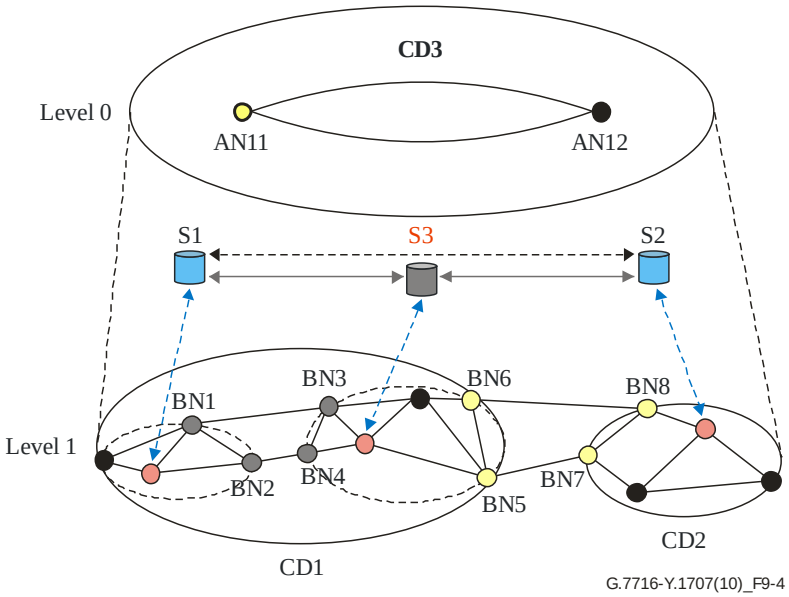

Figure 9-4 – Intermediate status

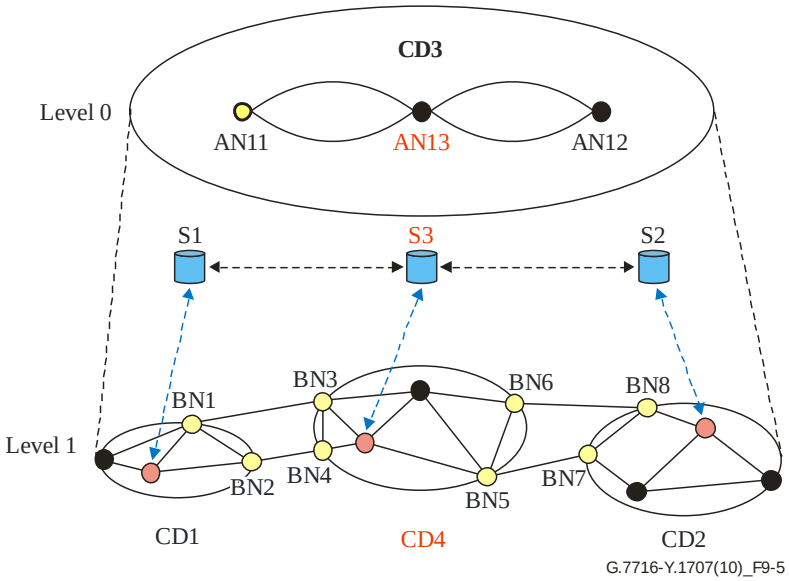

Figure 9-5 – After splitting

Different stages of routing area splitting are illustrated in Figures 9-3, 9-4 and 9-5. The procedures of routing area splitting can be summarized as follows:

1) Reconfigure AreaIDs of two splitting RAs after planning how to split the original RA. In general, one of the two splitting RAs may still have the original AreaID. For example, CD1 maintains the original AreaID in Figure 9-4.

2) Reconfigure routing controllers to advertise topology information associated with these two splitting RAs. For example, S3 is the new RC to represent new CD4 in level 1 and S1 still represents the left CD1.

3) Reconfigure routing controllers in adjacent routing control domains. For example, S3's neighbouring RCs are S1 and S2. S1's current neighbouring RC is S3 instead of S2.

4) Reconfigure inter-area links. For example, the links BN1-BN3 and BN2-BN4 are intra-area links in CD1 before splitting, but they should be configured as inter-area links in S1 and S3 after the routing area splitting.

5) Reconfigure intra-area links based on policy.

6) Reconfigure the reachable TRI on the corresponding RCs.

7) It is only necessary to reconfigure reference points, such as UNI, I-NNI, E-NNI. For example, the I-NNIs between BN1 and BN3, BN2 and BN4 before splitting should be reconfigured as E-NNIs after splitting. Policy should be also provided on these reference points.

8) Update the signalling state as needed.

Note that routing information feedup and feeddown may be reconfigured based on policy, and routing loop prevention should be considered in the case of multi-level routing hierarchy.

9.6.2.1.2 Routing area merging

The following example below shows the procedures of a single hierarchical level routing area merging.

During the process of routing area merging, an address conflict may happen when OSPF-TE synchronizes the databases of all routers, because two or more links may have the same address before merging. To avoid this conflict, the link addresses should be reconfigured either manually or automatically before the routing area merging process.

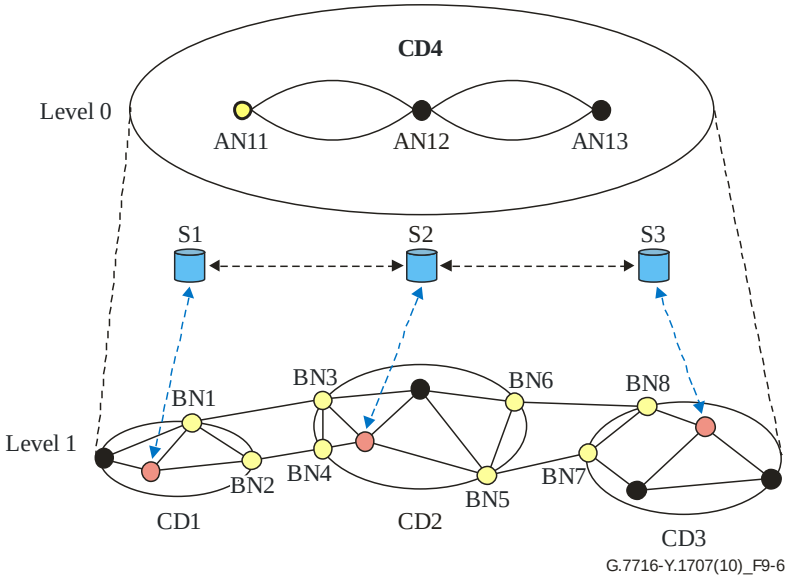

Figure 9-6 – Initial topology

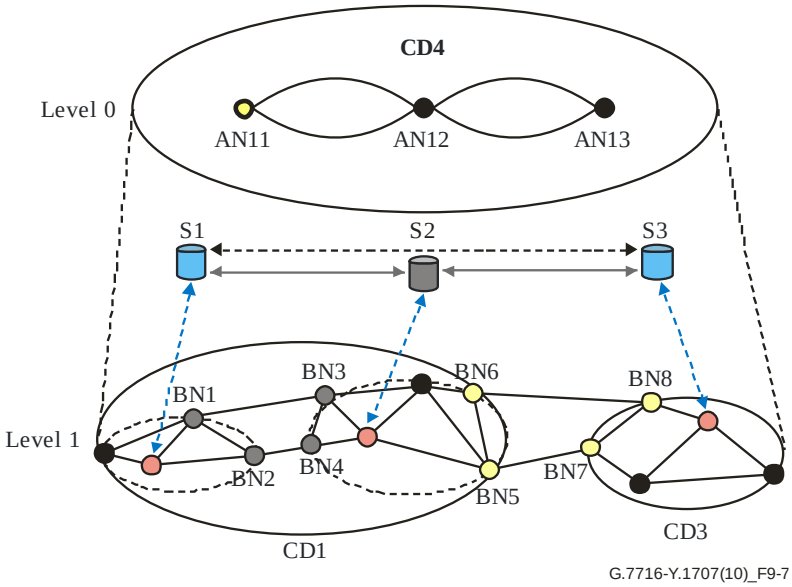

Figure 9-7 – Intermediate status

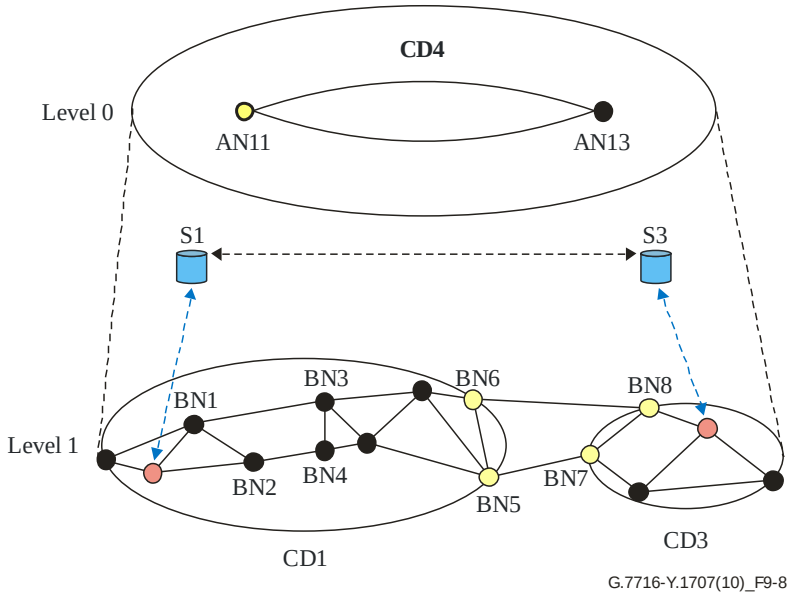

Figure 9-8 – After merging

The different stages of routing area merging are illustrated in Figures 9-6, 9-7 and 9-8. The procedures of routing area merging can be summarized as follows:

1) Reconfigure AreaIDs of two merging RAs, that is, the two merging routing areas should be reconfigured as the same AreaID.

2) Reconfigure routing controllers to advertise topology information associated with the merged routing area. For example, S1 will be reconfigured to represent new CD1 and the speaker function of S2 will be withdrawn.

3) Reconfigure routing controllers in adjacent routing control domains. For example, S1's current neighbouring RC is S3 instead of S2.

4) Reconfigure inter-area links. For example, the links BN6-BN8 and BN5-BN7 should be reconfigured as inter-area links on S1 and S3.

5) Reconfigure intra-area links based on policy. For example, the links BN1-BN3 and BN2-BN4 are inter-area links between CD1 and CD2 before merging, but these links should be reconfigured as intra-area links in CD1.

6) Reconfigure the reachable TRI on the corresponding RCs.

7) It is only necessary to reconfigure reference points, such as UNI, I-NNI, E-NNI. For example, the E-NNIs between BN1 and BN3, BN2 and BN4 before merging should be reconfigured as I-NNIs after merging. Corresponding policy should also be provided on these reference points.

8) Update the signalling state as needed.

Note that routing information fed up and fed down may be reconfigured based on policy, and routing loop prevention should be considered in the case of multi-level routing hierarchy.

9.6.2.2 Routing area creation/deletion

The general procedures for routing area creation and deletion are described in clauses 9.6.2.2.1 and 9.6.2.2.2.

9.6.2.2.1 Routing area creation

The example below shows the procedures for a single hierarchical level routing area creation.

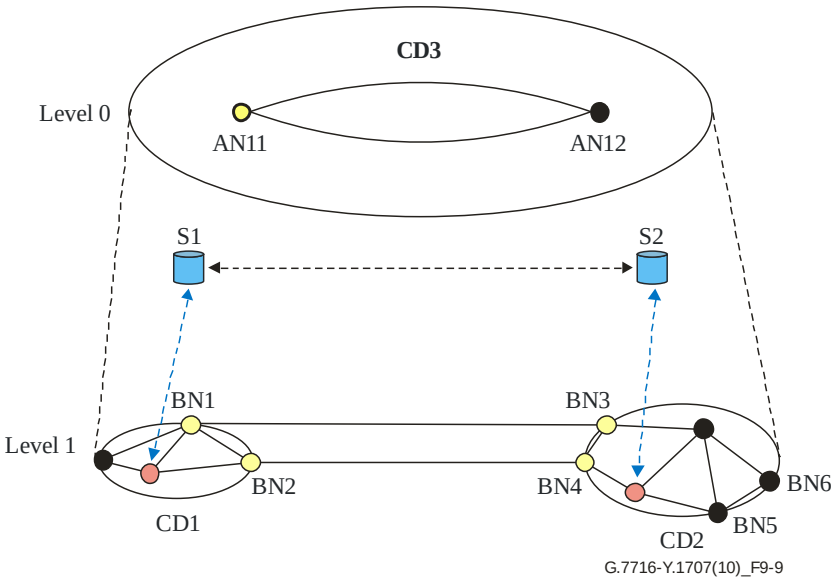

Figure 9-9 – Initial topology

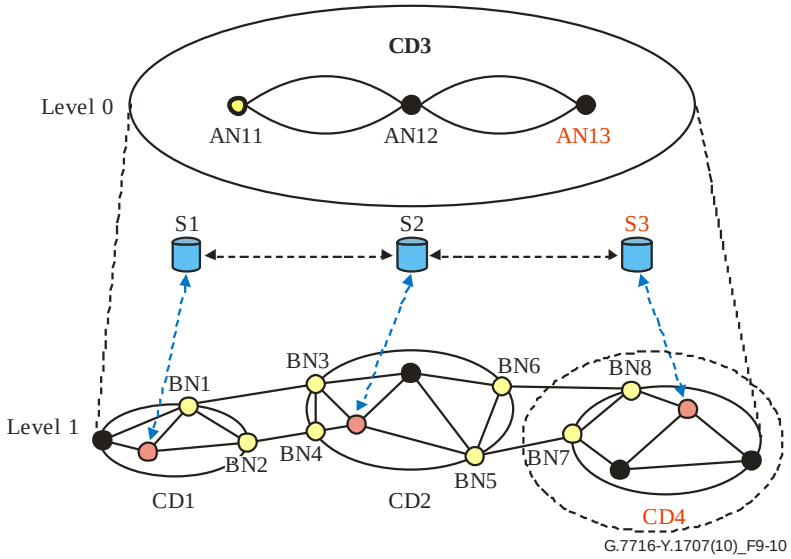

Figure 9-10 – Routing area attachment

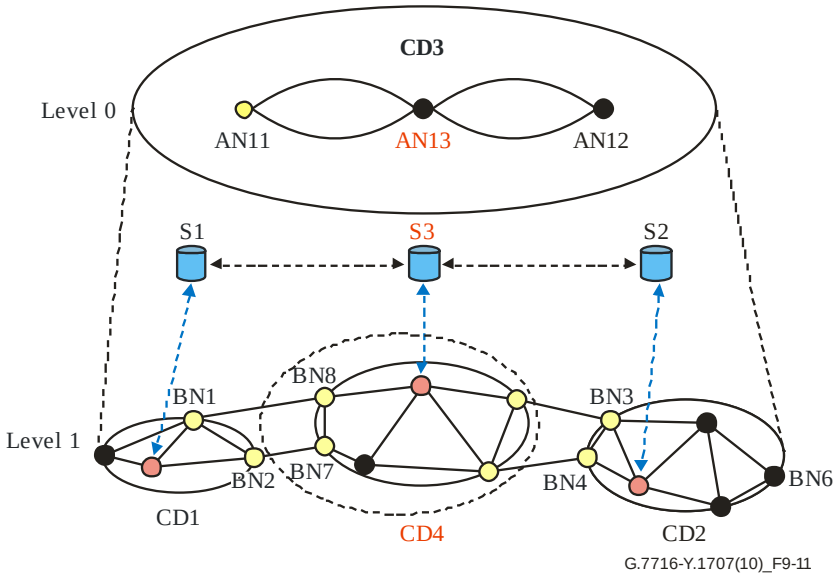

Figure 9-11 – Routing area creation

The procedures for routing area attachment or creation are similar to the procedures for routing area splitting. The procedures are described as follows:

1) Reconfigure AreaIDs of the creating routing area.
2) Reconfigure routing controllers to advertise topology information associated with the attaching routing area. For example, Figure 9-10 shows that S3 is the new RC to represent new CD4 in level 1.
3) Reconfigure routing controllers in adjacent routing control domains. For example, S2's neighbouring RCs are S1 and S3 in Figure 9-10.
4) Reconfigure inter-area links. For example, the links BN6-BN8 and BN5-BN7 should be configured as inter-area links in S2 and S3 in Figure 9-10.
5) Reconfigure intra-area links based on policy.
6) Reconfigure the reachable TRI on the corresponding RCs.
7) It is only necessary to reconfigure reference points, such as UNI, I-NNI, E-NNI.

8) Update the signalling state as needed.

Note that when a routing area is created between two routing areas (for example, in the case of Figure 9-11), the service provided by these two routing areas will be interrupted if the inter-area links are disconnected directly. So, the service should be rerouted before creation. However, the reconfiguration procedures of Figure 9-10 can also be applied to Figure 9-11.

9.6.2.2.2 Routing area deletion

The following example shows the procedures of a single hierarchical level routing area deletion.

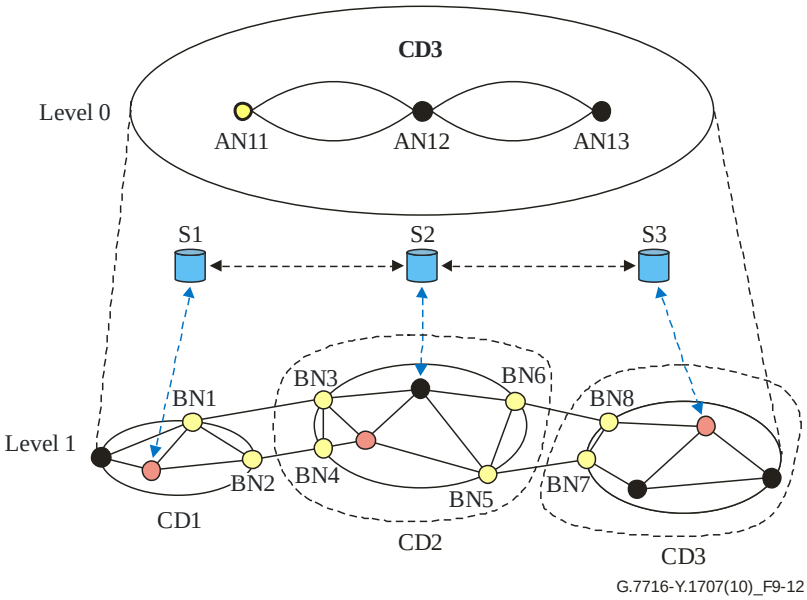

Figure 9-12 – Initial topology

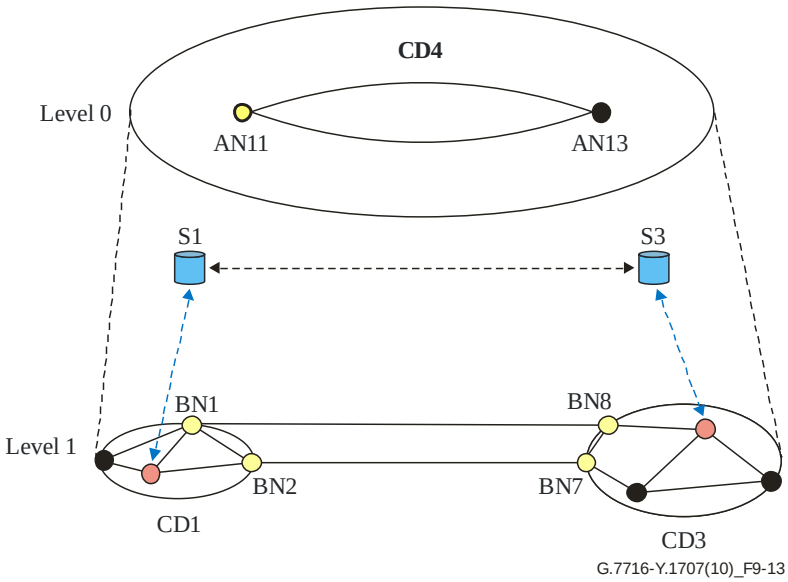

Figure 9-13 – After deletion (1/2)

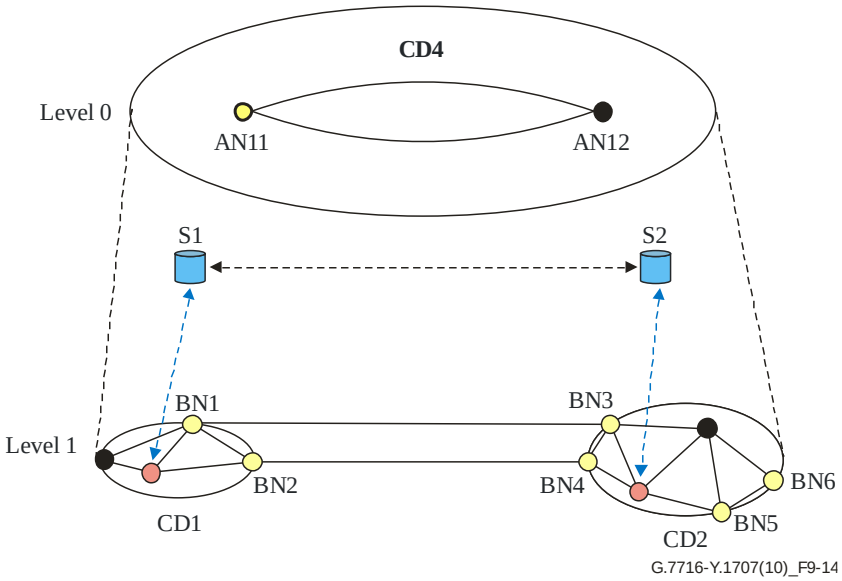

Figure 9-14 – After deletion (2/2)

The procedures for routing area deletion can be summarized as follows:

1) Reconfigure AreaIDs. In general, all the AreaIDs remain unchanged.
2) Reconfigure routing controllers to advertise topology information associated with the remained routing area. For example, S2 should be removed in Figure 9-13.
3) Reconfigure routing controllers in adjacent routing control domains. For example, S1's current neighbouring RC is S3 instead of S2 in Figure 9-13.
4) Reconfigure inter-area links. For example, the links BN1-BN8 and BN2-BN7 should be reconfigured as inter-area links on S1 and S3 in Figure 9-13.
5) Reconfigure intra-area links based on policy.
6) Reconfigure the reachable TRI on the corresponding RCs.
7) Update the signalling state as needed.

Note that when a routing area is deleted between two routing areas (for example, in the case of Figure 9-13), the service provided by these two routing areas will be interrupted if the routing area is deleted directly. So, the service should be rerouted before deletion. However, the reconfiguration procedures of Figure 9-13 can also be applied to Figure 9-14.

9.6.2.3 Strategy for routing area changes in SDN

In the SDN architecture, RC is a MC component in the controller. A general control neighbour relationship is built between the controller and all the nodes in the routing area. There are two types of routing control methods.

In the first method, all the nodes in a single routing area establish a neighbour relationship with the RC. Each node is directly controlled by the RC. Routing neighbour information is transmitted between RC and each single node. Figure 9-15 shows the first routing control method.

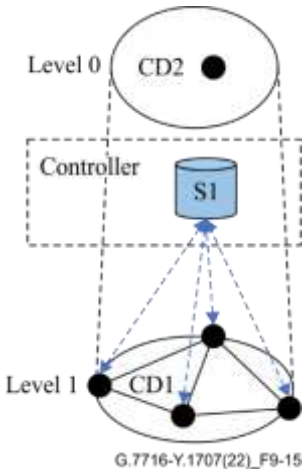

Figure 9-15 – Routing control method 1: RC builds routing neighbour relationship with all nodes

The second method is the same as the control method used in ASON architecture. A gateway node is selected to establish routing neighbour relationship with RC. The gateway node is responsible for collecting abstracted routing information of all nodes in the routing area. Routing information is transmitted between RC and the gateway node. The second method is usually used for reducing the amount of information processed b the controller and therefore improving the performance of the controller. Figure 9-16 shows the second routing control method.

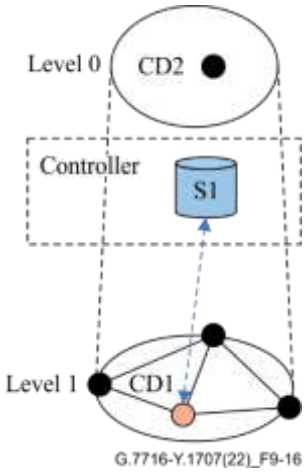

Figure 9-16 – Routing control method 2: RC builds routing neighbour relationship with gateway node

When splitting the routing area or inserting a new routing area, a neighbour relationship between the existing RC and the new RC needs to be reconfigured. There are two types of SDN architecture. One is the hierarchical architecture, and another one is the peer-to-peer architecture.

In the hierarchical SDN architecture, controllers of each single routing area are controlled by a centralized controller in the upper level. Topology information in a single routing area is collected by the corresponding RC. Links between lower-level RCs are in the scope of the upper-level controller. Routing neighbour information collected by lower-level RCs is conveyed to the upper-level RC. A neighbour relationship is not built between lower-level RCs. When splitting the routing area or adding a new routing area, the new RC only needs to build the routing neighbour relationship with upper-level RC. Scenario of routing area splitting in the hierarchical architecture is shown in Figure 9-17.

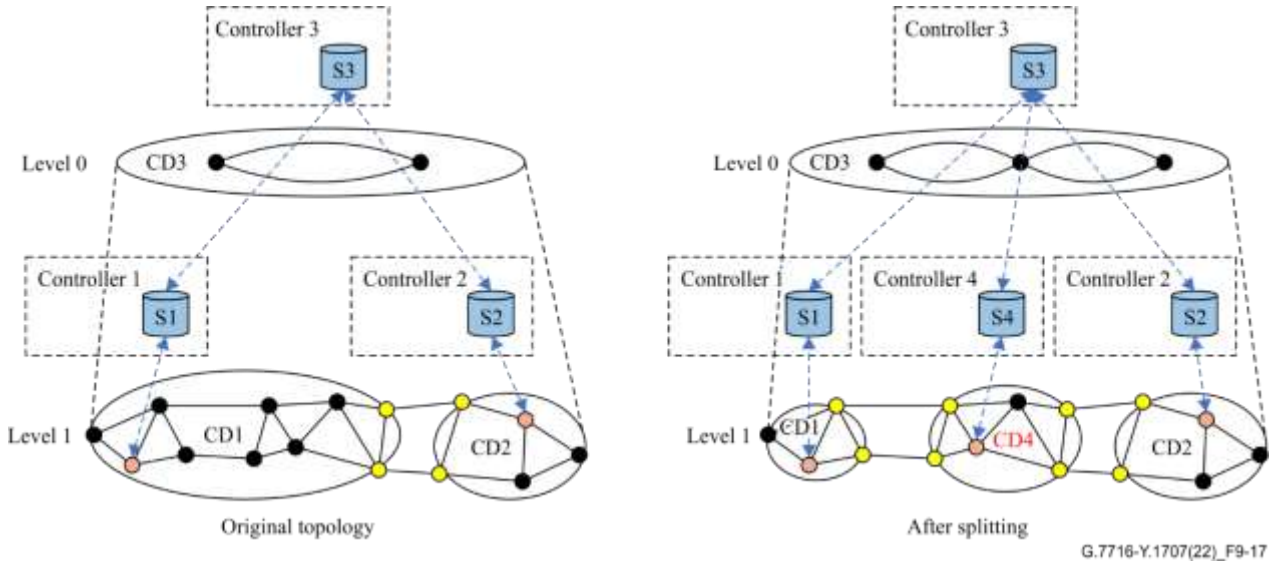

Figure 9-17 – Routing area splitting in hierarchical SDN architecture

In the peer-to-peer SDN architecture, a neighbour relationship is built between same level RCs. Routing information can be conveyed between same level RCs. In the peer-to-peer SDN architecture, when the routing area is split or a new routing area is added, the reconfiguration procedure followed by the same level RCs to establish the neighbour relationships is the same as procedure followed for the ASON architecture.

9.6.3 Strategy for control domain changes

In the process of operating networks, reconfigurations will be performed in a control domain. The reconfiguration of a control domain may be because of administrative or business reasons. There are four typical reconfigurations performed in control domain:

– Creation of client context;

– Deletion of client context;

– Creation of server context;

– Deletion of server context.

The following comments apply to the figures in this clause:

– Resources in level *n* that are marked in different colours are correspondingly mapped from level *n* – 1 controllers in the same colour. E.g., resources marked in orange are mapped from level *n* – 1 controller 1.

– A dash line implies a mapping relationship between resources in level *n* and resources in level *n* + 1. E.g., resources in level *n* + 1 controller 2 contain two parts which are respectively mapped from resources marked in orange and resources marked in green in level *n* controller 1.

– Although the resources are marked in different colours to indicate which controller they are mapped from, all the resources in the same local resource pool are anonymous.

9.6.3.1 Client context creation/deletion

The general procedures for client context creation and deletion are described in clauses 9.6.3.1 and 9.6.3.2.

9.6.3.1.1 Client context creation

When a new client is created, the corresponding client context is created. The example below shows the procedures for client context creation. See Figures 9-18 and 9-19.

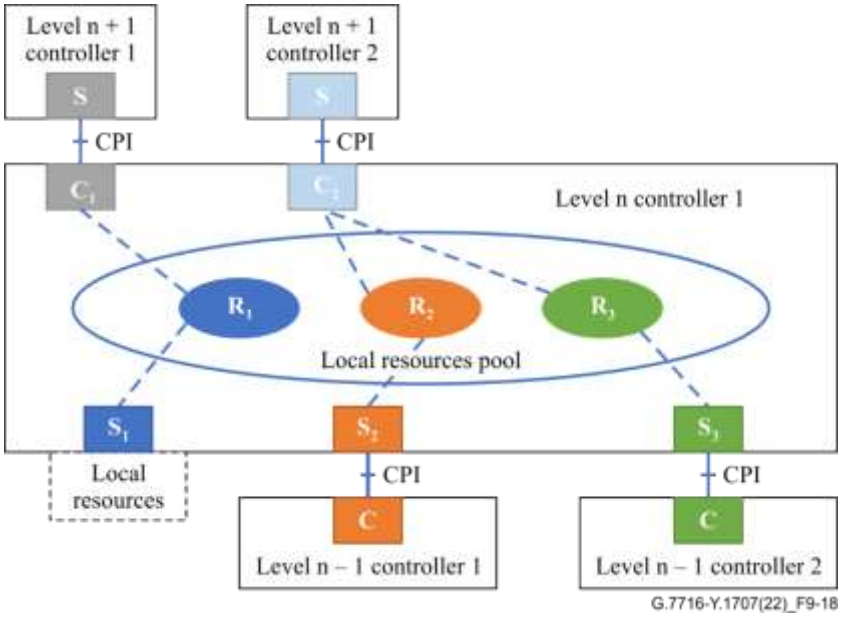

Figure 9-18 − Initial configuration of client context

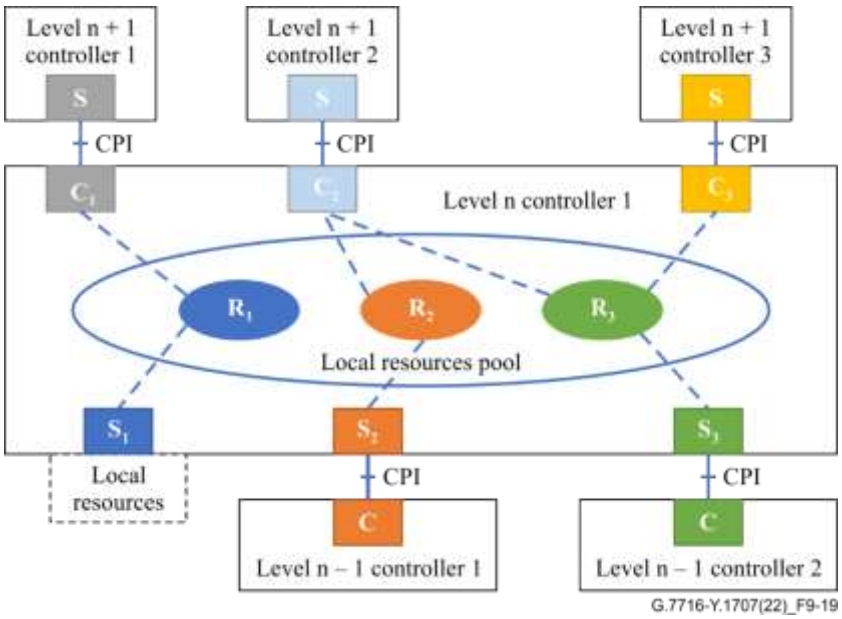

Figure 9-19 − Client context creation

The procedures for client context creation can be summarized as follows:

1) The level *n* + 1 controller 3 is created.
2) The client context for level *n* + 1 controller 3 mapped from level *n* controller 1 is created.
3) Neighbour relationship between level *n* controller 1 and level *n* + 1 controller 3 is created.

9.6.3.1.2 Client context deletion

When all the business activities of a client have ended, this client and the corresponding client context need to be deleted. The example below shows the procedures for client context deletion. See Figures 9-20 and 9-21.

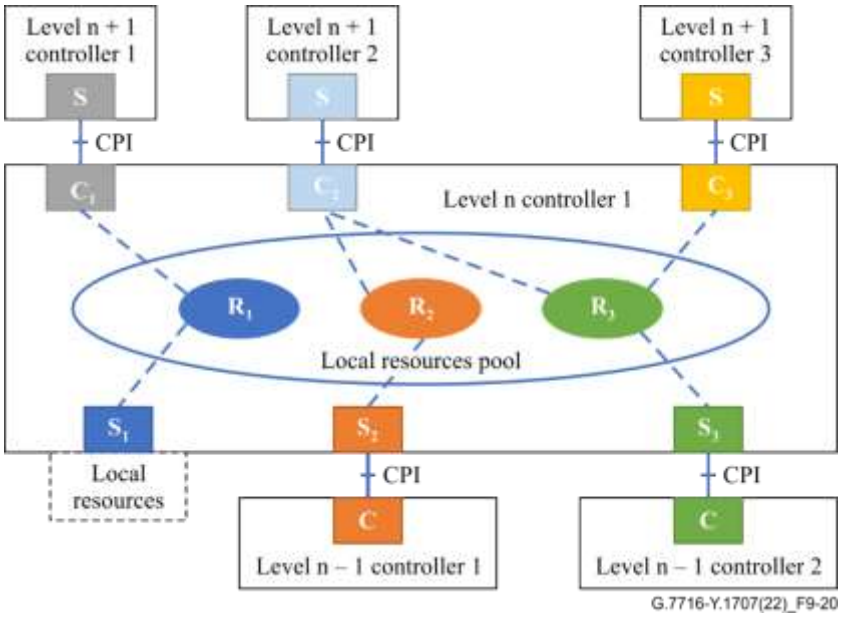

Figure 9-20 − Initial configuration of client context

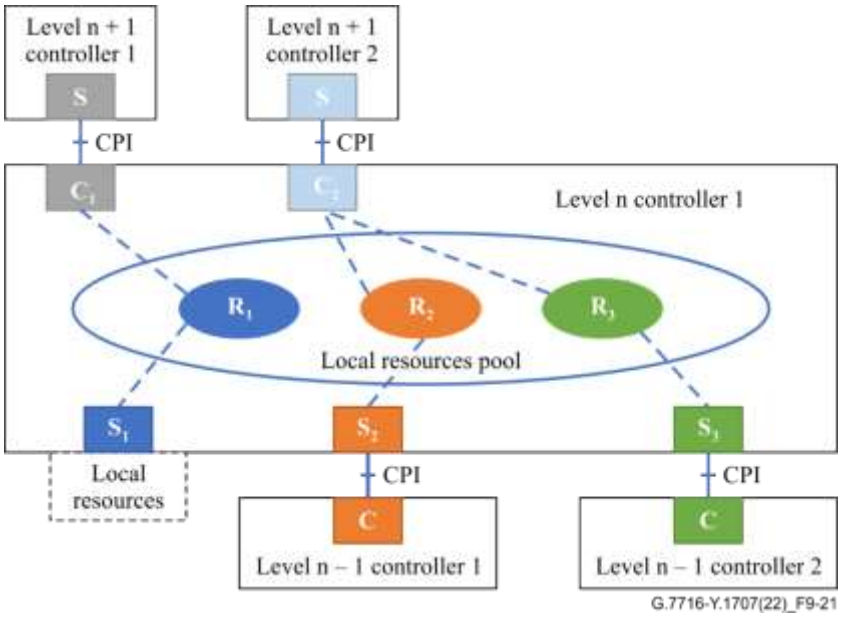

Figure 9-21 − Client context deletion

The procedures for client context deletion can be summarized as follows:

1) The level *n* + 1 controller 3 is deleted.
2) The client context for level *n* + 1 controller 3 mapped from level *n* controller 1 is deleted.
3) Neighbour relationship between level *n* controller 1 and level *n* + 1 controller 3 is deleted.

9.6.3.2 Server context creation/deletion

The general procedures for server context creation and deletion are described in clauses 9.6.3.2.1 and 9.6.3.2.2.

9.6.3.2.1 Server context creation

When resources in a lower level need to be used by an upper level client, the corresponding server context for the lower level controller is created. Figures 9-22 and 9-23 depict the procedures for server context creation.

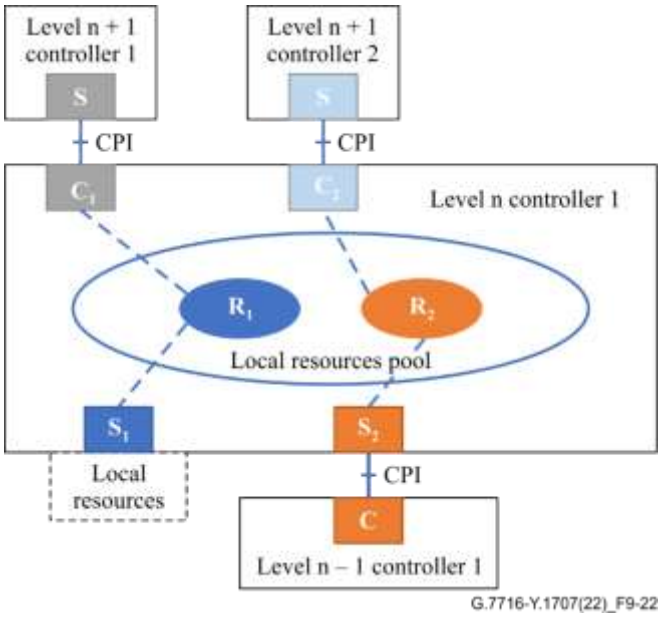

Figure 9-22 − Initial configuration of server context

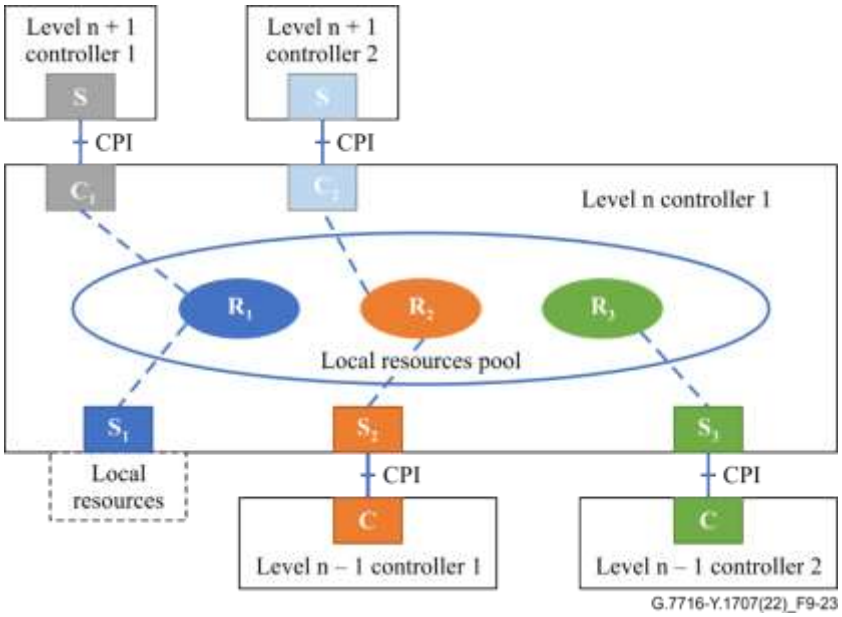

Figure 9-23 − Server context creation

The procedures for server context creation can be summarized as follows:

1) The level *n* – 1 controller 2 is created.
2) The server context for level *n* – 1 controller 2 mapped from level *n* controller 1 is created.

3) Neighbour relationship between level *n* controller 1 and level *n* – 1 controller 2 is created.

4) Resources mapped from level *n* – 1 controller 2 are created in local resource pool of level *n* controller 1.

9.6.3.2.2 Server context deletion

When resources in a lower level are not used by an upper level client, the corresponding server context for the lower level controller need to be deleted. Figures 9-24 and 9-25 depict the procedures for server context deletion.

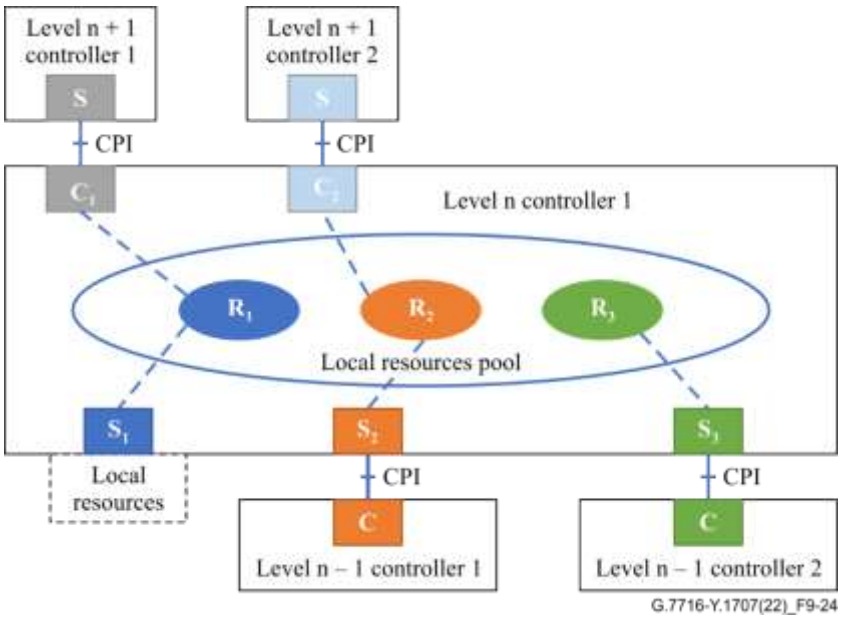

Figure 9-24 − Initial configuration of server context

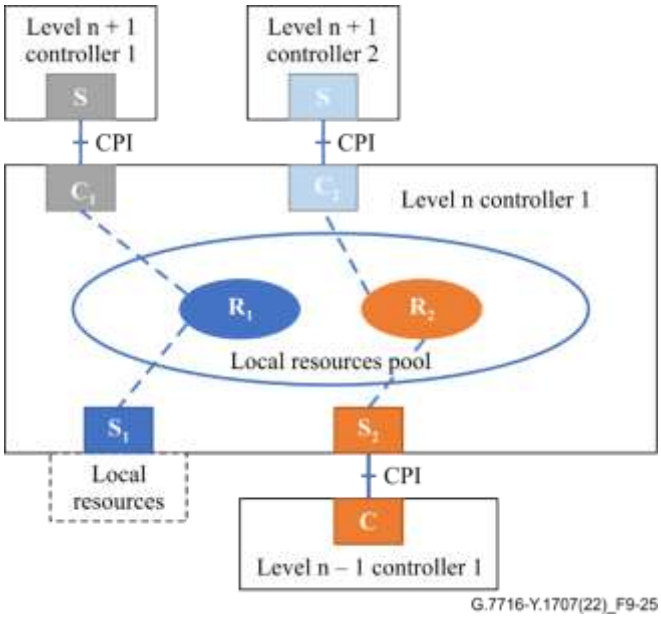

Figure 9-25 − Server context deletion

The procedures for server context deletion can be summarized as follows:

1) The level *n* – 1 controller 2 is deleted.

2) The server context for level *n* – 1 controller 2 mapped from level *n* controller 1 is deleted.

3) Neighbour relationship between level *n* controller 1 and level *n* – 1 controller 2 is deleted.

4) Resources mapped from level *n* – 1 controller 2 are deleted in local resource pool of level *n* controller 1.

9.7 Auditing

The auditing process is applied to the transport resources; this is not a one-time process, i.e., not only done at initialization/restart time but also done at running time (periodically, manually triggered or event triggered). The auditing process includes checking the consistent views of the relevant transport resources between the control domain and the MC within one node; it also includes checking the consistent views of the relevant transport resources between the control domain peers of the neighbouring nodes.

The auditing process can be triggered by certain events during the running time, these events may include:

– Connection set-up failure occurs because of the inconsistent view of the transport resource between the control domain and the transport resource.

– Inconsistency between control domain peers is detected.

– Inconsistency between control domain and transport resource is detected.

− Inconsistency between transport resource in MC components of different levels.

Whenever an inconsistency is detected, it should either be resolved, or an alarm should be raised if operator intervention is needed. However, transient inconsistency, e.g., occurring during connection set-up, should not lead to an alarm.

9.7.1 Between MC and transport resources

In a same node, for the same transport resource, the control domain should have a view consistent with that of the MC. The status of the transport resources should be represented correctly by the control domain and the MC.

9.7.1.1 Resource state

When an SNP is assigned by the MC to the control domain, the control domain needs to be provided with the current state of the SNP. After assignment, change in the SNP state should only occur as the result of control domain action.

During the auditing process, the status of the transport resources is exchanged between control domain and transport resource, if any inconsistency is detected for resources that have been assigned to the control domain, the control domain should not use the SNP resource (i.e., set the SNP state of the resource to "busy") and notify the MC.

The interface that provides this indication is for further study.

9.7.2 Between MC peers and hierarchies

Between the neighbouring nodes, the control domain peers should have a consistent view of the transport resources.

9.7.2.1 SNP state

When a transport link connection is allocated to support the SNP link connection, the state of the SNP pairs of the SNP link connection should be consistent.

During the auditing process, the SNP state of the remote end of the link connection is received and compared with that of the local end. According to the auditing result, the LRM knows if a transport link connection can be allocated to support the SNP link connection. If any inconsistency is detected

for resources that have been assigned to the MC system, the supporting MC system should report to the leading MC system.

The interface that provides this indication is for further study.

9.7.3 Link consistency check

9.7.3.1 Overview

The purpose of the link consistency check is to describe which link attribute may be verified, the action taken by the MC systems in the consistency check phase and what should be done when the consistency check is finished. There is a difference in different link attribute consistency checks. The different MC systems should cooperate with each other to finish link attribute consistency checks. The consistency check should only be invoked after both ends of the link have been configured to avoid "transient mismatches".

9.7.3.2 Content to be verified

There are two kinds of link attribute that may be verified:

1) Attribute configured by leading system. This attribute may include link metric, link protection type, etc.
2) Link bandwidth information. This attribute may include available bandwidth and distribution of assigned resources, etc.
3) Correct association of SNP link connection endpoints.

A consistency check of link bandwidth information means that the information of the local end (output for local node) of a link is in conformity with that of the remote end (input for local node) and vice versa. Because of the existence of unidirectional service, it is not necessary to verify the bandwidth information of the input and output of the local end.

A consistency check of link metrics does not require that the local and remote ends have the same value.

9.7.3.3 Consistency check mode of link attributes

The process of the link attribute consistency check is as follows:

1) The node on one side of the link which is to be verified collects attributes configured by the leading system and bandwidth information and sends them to the remote node to request it to verify them with the corresponding information stored on that node.
2) On the other hand, this node may receive consistency check requests from remote node and then verify the input information with that stored on this node.

But the start-up of consistency checks is different for different kinds of link attribute. The link attribute configured by the leading system can be modified by the leading system and the supporting system starts to verify the modified link attribute after it processes the modification request.

For link bandwidth information, which may change during to resource partition or service set-up/cancel, users should start the consistency check manually with the leading system at the appropriate time.

9.7.3.4 Report of consistency check result

The consistency check result should be reported according to the decision of the operator. If it is matched, the supporting system should report success to the leading system. If there is any mismatch in the consistency check, corresponding alarm information should be reported to the leading system and an additional process should be taken, as follows:

1) If there is any mismatch in the consistency check of a link attribute configured by the leading system, users can reconfigure the link attribute and then to trigger the supporting system to start to verify it again.

2) If there is any mismatch in the consistency check of the link bandwidth information, the mismatched resources should be masked to avoid being used by a new service, and at this time, the alarm information should not be produced in the next consistency check.

9.8 Recovery

During the operation of the control domain, various fault conditions might occur. The ASON architecture described in clause 12 of [ITU-T G.7703] provides guidance for recovery of the control domain from these conditions.

At the initialization phase of the control domain recovery process, the relevant MC components should be aware of the system recovering from a fault condition, which results in the control domain state re-synchronization process. The control domain state (which includes the transport resource and SNC state information, and the soft state of control domain signalling sessions) can be recovered from the transport resource and MC, as well as the control domain state of the remote MC components.

A vertical consistency check is performed between the control domain, transport resource and MC. A horizontal consistency check is performed between local and remote MC components.

Based on different fault conditions, a set of functional components may perform the recovery process. For example, power cycling a board will trigger all the functional components which reside on that board to perform the recovery process.

10 Operation on virtual networks

[ITU-T G.7701] puts forward the concept of a VN and a procedural description is given in [ITU-T G.7702]. When the transport resources are virtualized and shown in upper layer MC systems, they are represented as a VN. The operation and maintenance of VN are also required in the network. Furthermore, the network slicing technology is highly dependent on the VN provisioning, and the corresponding management functions would be needed as well.

MCS maintains the resource information SNPP links in its management and control domain.

After receiving a request from a client, the administrator of the MCS creates a client context according to the different policies and selection criteria established for the client. Then, based on the virtualization method described in [ITU-T G.7702], the administrator of the MCS constructs the VN and maintains the identifier name space mapping between the local and client contexts. The VN topology information of each client is maintained independently. VN resources are only exposed to the corresponding VN controllers.

In addition, the MCS also manages the lifecycle of the VN. A VN is a part of the information contained in a client context or a server context, and its lifecycle depends on the lifecycle of the client/server context. When receiving a request (for example, capacity expansion or topology change) from a client, the MCS reconfigures the VN without adding/removing physical network resources. When a client context is deleted, the VN is deleted, the dedicated virtual network resources of the client are deleted, and the corresponding SNPs and forwarding points (FPs) in the transport resources are released.

10.1 VN resource assignment

VN resource allocation during the startup of the controller is shown in Figure 10-1. The procedure can also be applied for VN resource assignment in [ITU-T G.7716].

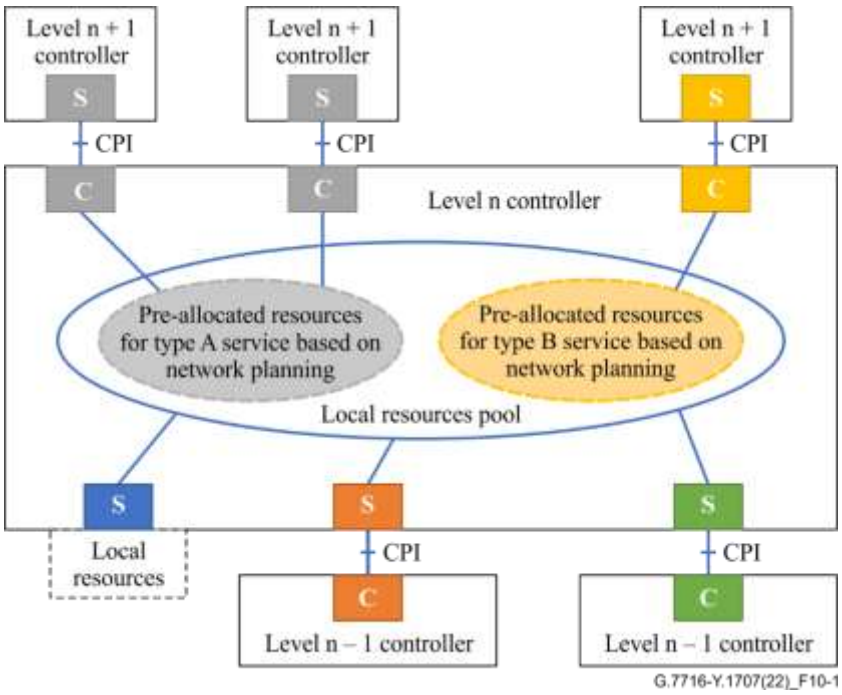

Figure 10-1 − Transport network resource assignment for VN

1) Resource assignment for server context

The server context is composed of the transport resources from local planning and lower level MCs. The resources scope of the MC is determined by the server context.

2) Resource assignment for client context

The controller can allocate network resources in advance, before the customer requirements are received. Different resource groups can be formed and pre-allocated to satisfy different service types, shown as type A and type B in Figure 10-1. Service types can be defined based on the following strategies:

− Applications, such as enterprise customer, 5G base station, etc.;

− SLA consideration, such as delay requirements, isolation requirements, etc.;

− Other manual strategies.

Resources in the pool can be divided according to service type.

10.2 VN name mapping

Within the same controller, the naming mapping relationship between server context, local resources pool and client context is as follows:

− The resource in server context are mapped and generated to the local resources pool. The resource in the server context and the local resources pool are a one-to-one relationship and consistent, but their name space may be different. For example, the naming in the local resources pool can be prefixed to distinguish that the resource comes from different server contexts, such as resource N1 in server context 1, its mapped resource ID in local resources pool is S1.N1, as shown in Figure 10-2**Error! Reference source not found.**.

− For resources that are shared by multiple client contexts, a separate resource alias is formed in each client context. The SNP in the local resources pool is mapped or virtualized to the SNPP in the client context.

− For resources that are dedicated to a specific client context and not shared with others, the lower-level SNP or SNPP in the local resources pool can be mapped or virtualized to the SNPP in the upper-level client context.

− For abstract nodes or other virtualized resources, network resources aliases need to be configured.

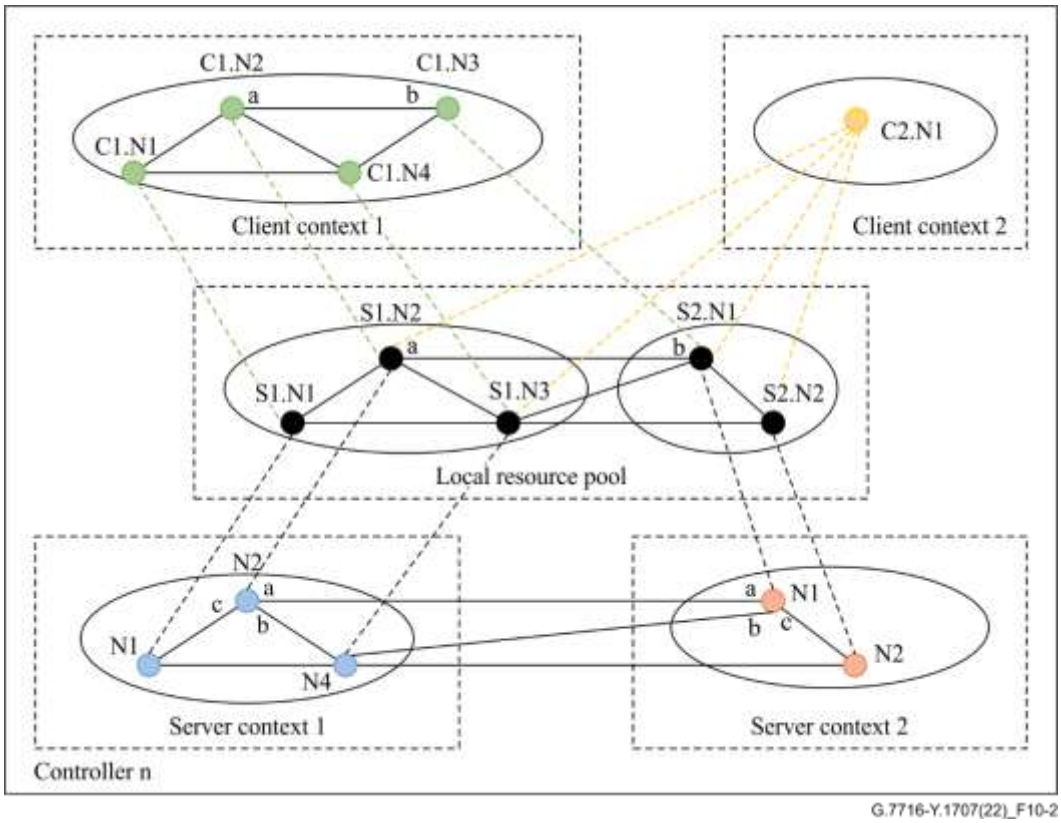

Figure 10-2 − Name mapping for server context and client context in VN

Between different controllers, the name space mapping between the server context and the client context can be realized through resource query, reporting, discovery and other mechanisms, and the namespace between them should be consistent. If the hierarchical controllers are in a trusted relationship, name mapping may not be required.

10.3 VN reconfiguration

When transport resources with FP namespace directly visible are added or removed, the (re)allocation of the lower-level transport resources may impact the content of the server context based on the objectives of planning. Six typical scenarios are described in clauses 10.3.1 and 10.3.2. These scenarios can basically be divided into two types. In the first type, the (re)allocation of resources only impact the local resources pool, but does not impact any client context (i.e., more or less transport resource available in the pool). In the other type of scenarios, the (re)allocation of resources will cause the change of client context due to the optimization of resource allocation.

10.3.1 Scenarios where the client context is not impacted

In some scenarios, changes of lower-level transport resources do not impact the higher-level client context. Four scenarios are described as follows:

1) When transport resources with FP namespace visible are added, the content of the higher-level client context is not impacted after the resource adjustment of the server context. In this case, the new transport resources are available only in the local resources pool, but not the client context. See Figure 10-3.

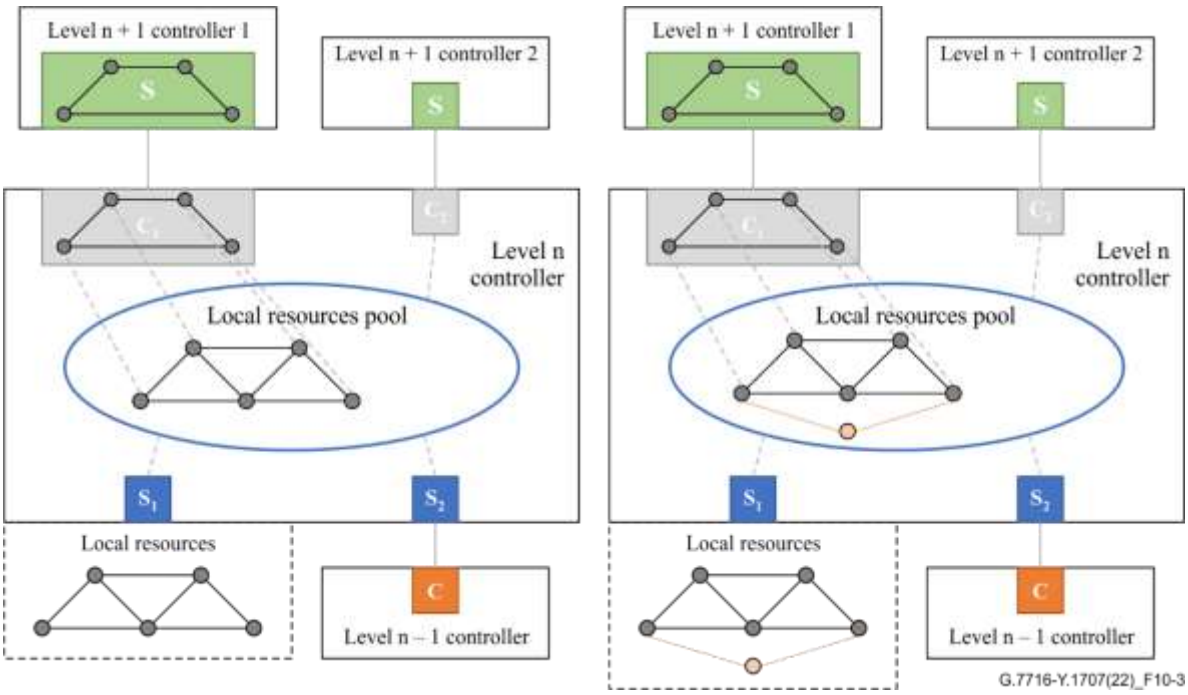

Figure 10-3 − Local resource added and client context not impacted

2) When an FP namespace visible resource is not allocated to any higher-level client, it can be deleted. See Figure 10-4.

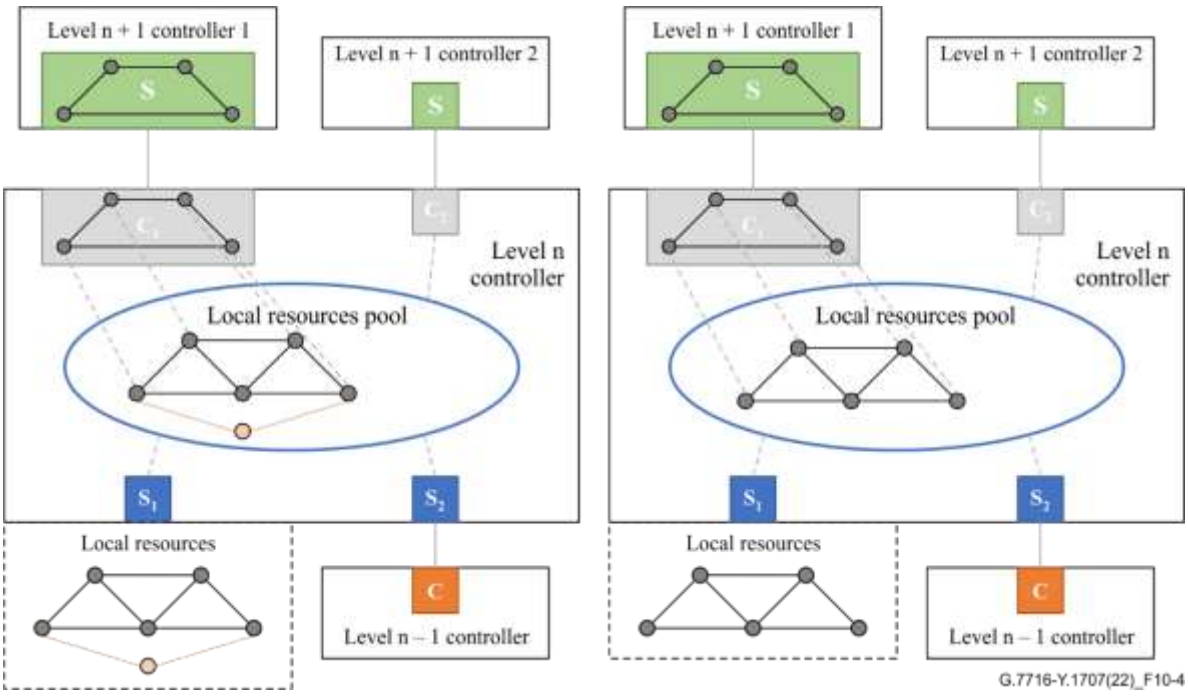

Figure 10-4 − Local resource deleted

3) When a new controller with additional resources is added as a subordinate, resources are mapped into the local resources pool via a new server context for this new controller. Meanwhile, links between resources that came from different server contexts are mapped into the resources pool. The content of the higher-level client context is not impacted by the addition of the server context. See Figure 10-5.

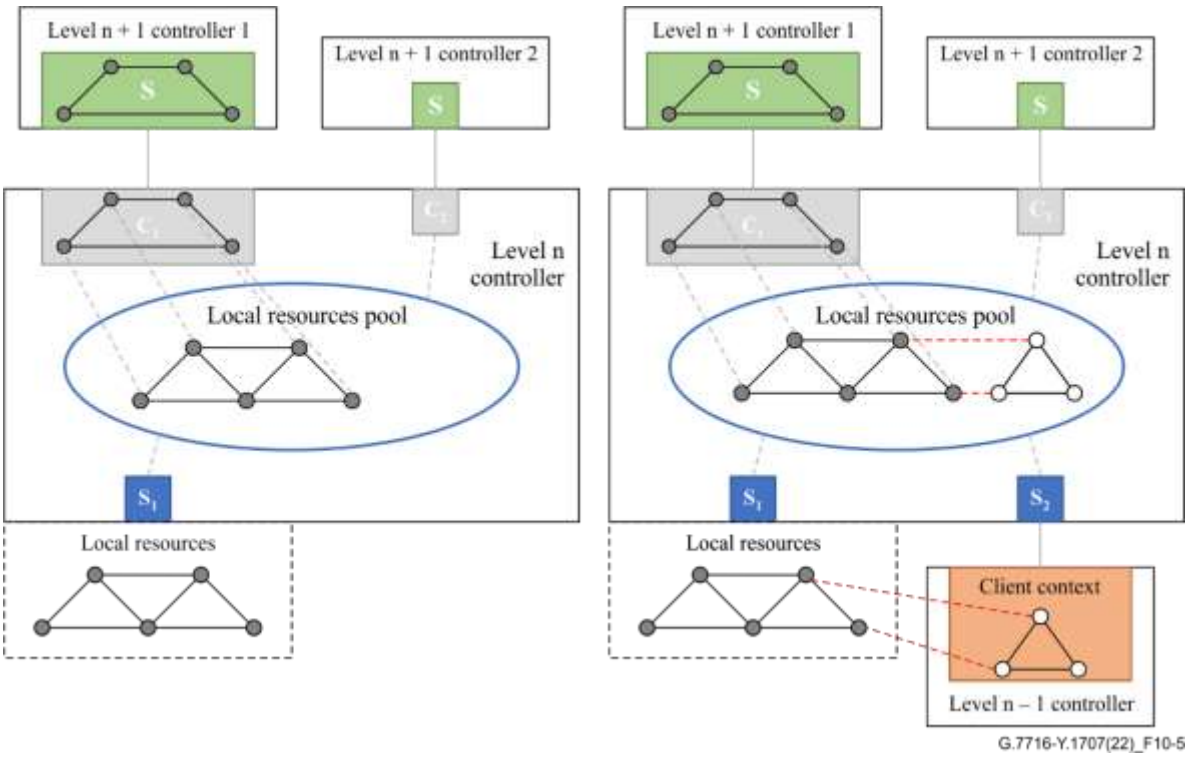

Figure 10-5 − Controller added and client context not impacted

4) When resources in a lower-level controller are not used by the upper-level client, the controller can be deleted. For example, in Figure 10-6 the orange link in the local resources pool is no longer used by client context C1 as backup, the resources from S2 can be deleted. Meanwhile, links between resources came from different server contexts are deleted. See Figure 10-6.

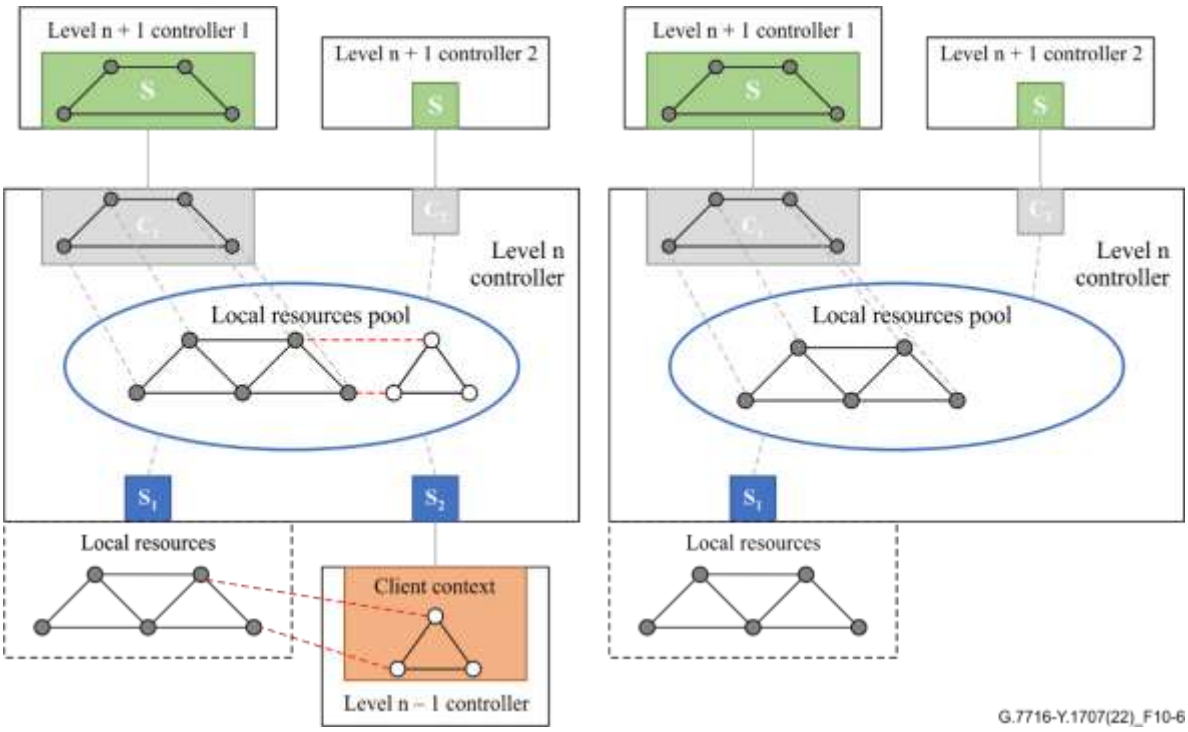

Figure 10-6 − Controller deleted

10.3.2 Scenarios where the client context is impacted

In some scenarios, changes of lower-level transport resources cause optimization of the upper-level client context. In these cases, the optimization suggestion is given to the client, and it is the client who makes the decision whether the optimization should be made. Two scenarios are described as follow:

1) When a physical resource is added, an optimization routing scheme is provided to the client when the SLA changes. Typical scenarios include bandwidth addition, protection relationship changing, route switching, etc. If the client agrees to make the optimization, the content of the upper-level client context is correspondingly adjusted for the optimization purpose. The mapping relationship changes as well. See Figure 10-7.

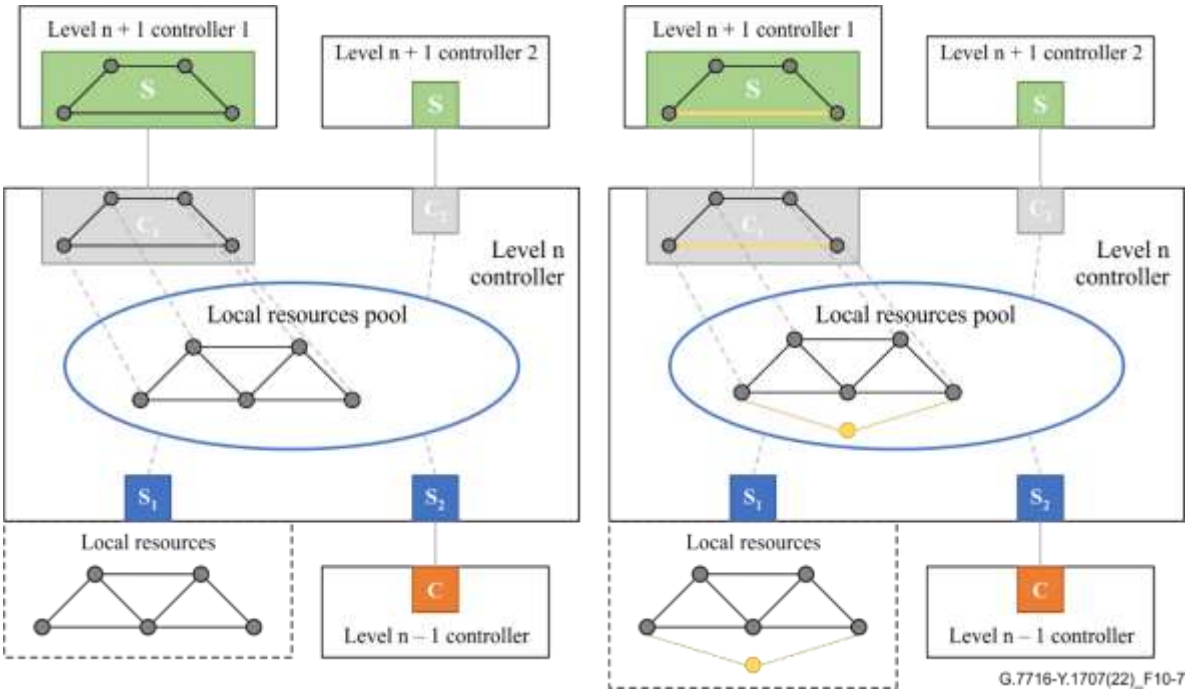

Figure 10-7 − Local resource added and client context impacted

2) When resources in a new controller is added, resources are mapped into the local resources pool. Meanwhile, links between resources that come from different server contexts are mapped into the resources pool. An optimization routing scheme is provided to the client when the SLA changes. Typical scenarios include bandwidth addition, protection relationship changing, route switching, etc. If the client agrees to make the optimization, the content of the upper-level client context is correspondingly adjusted for the optimization purpose. See Figure 10-8.

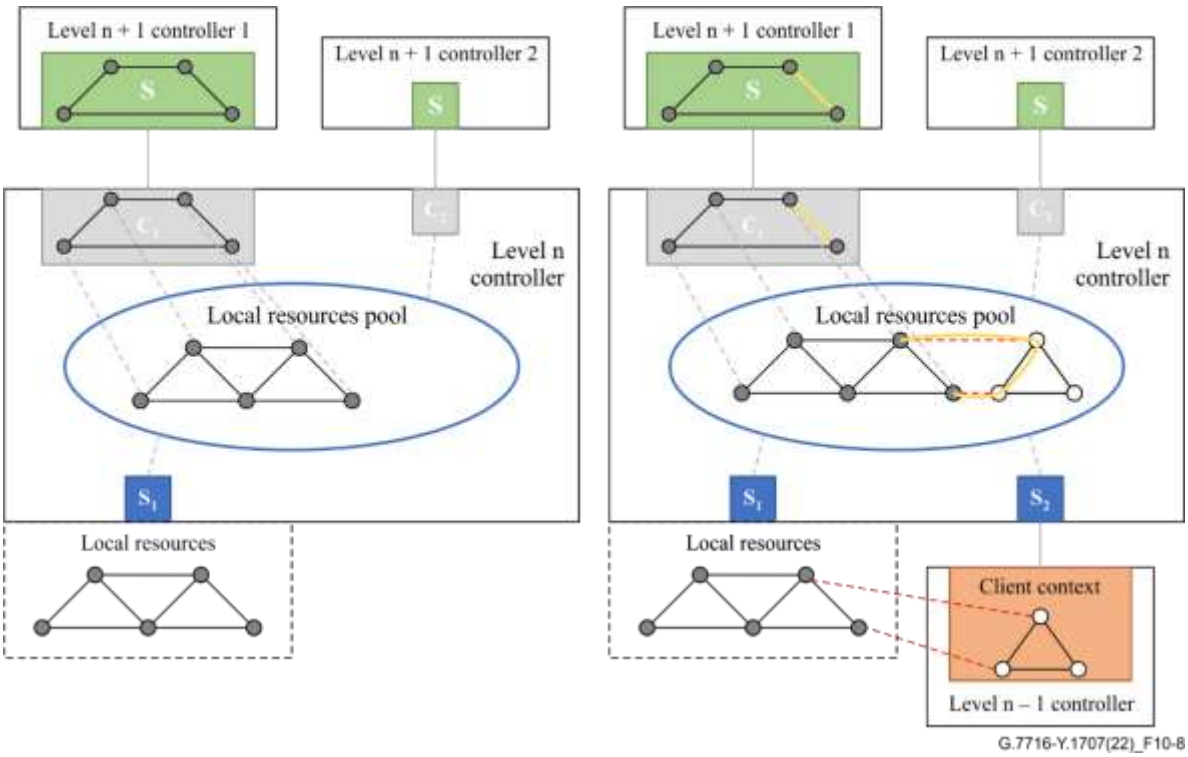

Figure 10-8 − Controller added and client context impacted

Appendix I

Initialization example

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

The start-up sequence of the MC components is based on the components' dependency relationships, so the depended-on components should be initialized prior to the dependent components. The binding of the MC components may be controlled by a centralized functional component such as "system initialization", or may be achieved through some automatic distributed approach.

An example process of the control domain initialization is illustrated in Figure I.1:

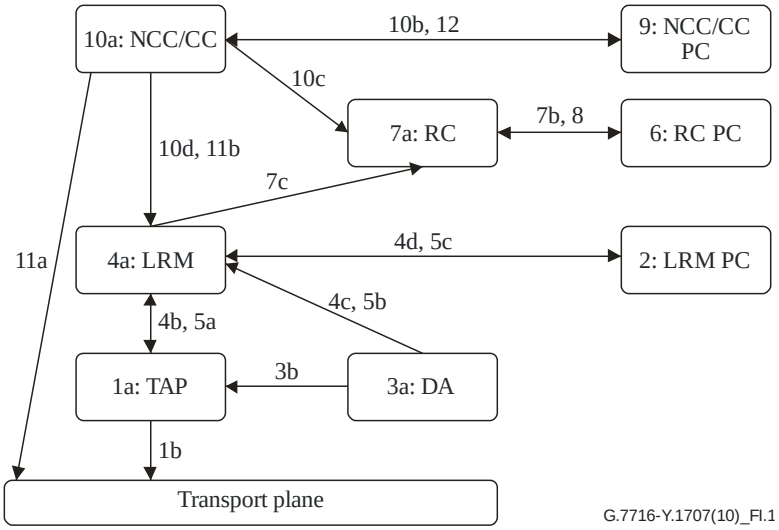

Figure I.1 – Control domain initialization process

1) Start of the termination and adaptation performer (TAP) component. It gets connection point (CP) information (e.g., CP name, signal type, bandwidth and CP status) from transport resource. Then TAP will be informed of CP-SNP relationship.

2) Start of the signalling protocol controller (PC) component. It gets LRM ID and signalling PC SCN address information from permanent storage to establish the relationship of LRM ID and signalling PC SCN address.

3) Start of the DA component. It associates itself with TAP component and discovers CP link connections within the transport name space.

4) Start of the LRM component. It associates itself with TAP, DA and signalling PC components, and gets area ID and node ID, etc., from permanent storage.

5) LRM gets SNP and SNP status from TAP component, and then gets SNPP link connection information (such as the local area ID, node ID, SNPPID, bandwidth, SRLG, etc., and the corresponding information of remote/peer nodes) from permanent storage. LRM component will communicate with peer LRM component to discover SNP/SNPP link connections.

6) Start of the signalling PC component. It gets RC ID and signalling PC SCN address information from permanent storage to establish their binding relationship.

7) Start of the RC component. It associates itself with LRM, signalling PC components, and gets area ID and node ID, etc., from permanent storage. RC component will get local SNP/SNPP link connections from local LRM component.

8) The RC component communicates with peer RC components to synchronize network topology information.

9) Start of the signalling PC component. It gets NCC/CC ID and signalling PC SCN address information from permanent storage to establish their binding relationship.

10) Start of the NCC/CC component. It associates itself with signalling PC, RC and LRM components and gets NCC/CC ID information from permanent storage.

11) CC component coordinates other components (such as LRM, TAP) to verify the cross-connection status between control domain and transport resource after CC gets link connection information from permanent storage. If any status inconsistency is found, an alarm will be raised, and an event will be reported to the MC to take further action.

Bibliography

[b-ITU-T X.638] Recommendation ITU-T X.638 (1996), *Minimal OSI facilities to support basic communications applications*.

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