International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# G.7716/Y.1707

(01/2010)

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 AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Operation, administration and maintenance

---

## Architecture of control plane operations

Recommendation ITU-T G.7716/Y.1707

ITU-T

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 control plane operations


### Summary

Recommendation ITU-T G.7716/Y.1707 addresses the architecture of control plane operations. Guidance for service providers on the automatically switch optical network (ASON) network plan, performing typical operations in the network, and sequencing the ITU-T G.7718.1 operations, are described in this Recommendation. This Recommendation also provides guidance to control plane function and protocol designers on the sort of operations control plane protocols and implementations that they need to be able to support.



### History

| Edition | Recommendation | Approval | Study Group |
|---|---|---|---|
| 1.0 | ITU-T G.7716/Y.1707 | 2010-01-13 | 15 |

## 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

# CONTENTS

# Recommendation ITU-T G.7716/Y.1707

## Architecture of control plane operations

### 1 Scope

This Recommendation provides guidance for the service providers on:

– how to plan an automatically switched optical network (ASON) network;

– the actions necessary to perform typical operations in the network;

– how to sequence the ITU-T G.7718.1 operations.

This Recommendation also provides guidance to control plane function and protocol designers on the sort of operations control plane protocols and implementations that 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.798] Recommendation ITU-T G.798 (2006), *Characteristics of optical transport network hierarchy equipment functional blocks*.

[ITU-T G.872] Recommendation ITU-T G.872 (2001), *Architecture of optical transport networks*.

[ITU-T G.7710] Recommendation ITU-T G.7710 /Y.1701 (2007), *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.7713] Recommendation ITU-T G.7713/Y.1704 (2009), *Distributed call and connection management (DCM)*.

[ITU-T G.7713.1] Recommendation ITU-T G.7713.1/Y.1704.1 (2003), *Distributed Call and Connection Management (DCM) based on PNNI*.

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

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

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

[ITU-T G.7714.1] Recommendation ITU-T G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*.

| | |
|---|---|
| [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.7715.2] | Recommendation ITU-T G.7715.2/Y.1706.2 (2007), *ASON routing architecture and requirements for remote route query*. |
| [ITU-T G.7718] | Recommendation ITU-T G.7718/Y.1709 (2005), *Framework for ASON management*. |
| [ITU-T G.7718.1] | Recommendation ITU-T G.7718.1/Y.1709.1 (2006), *Protocol-neutral management information model for the control plane view*. |
| [ITU-T G.8080] | Recommendation ITU-T G.8080/Y.1304 (2006), *Architecture for the automatically switched optical network (ASON)*. |
| [ITU-T G.8081] | Recommendation ITU-T G.8081/Y.1353 (2008), *Terms and definitions for Automatically Switched Optical Networks (ASON)*. |

# 3 Definitions

## 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 platform** (ITU-T X.638): An implementation of an identified platform specification.

**3.1.2 platform specification** (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 plane instance. These parameters are fundamental to the continued operation of the control plane instance and cannot be changed without significant impact to the control plane instance. Therefore, Commissioning is only done during the initialization phase of the control plane lifecycle. Note that commissioning is focused on the commissioning on the control plane component and not the data/transport plane resource.

**3.2.2 provisioning**: The act of specifying the parameters necessary when assigning/deassigning network resources to/from the control plane or to invoke/remove services provided by a control plane instance. These parameters are specific to a resource or service request, causing changes to these parameters to only impact a specific resource or service request. Therefore, provisioning is allowed in the initialization and operations phases of the control plane lifecycle.

# 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 |
| CP | Control Plane |
| DA | Discovery Agent |
| DCN | Data Communication Network |
| E-NNI | External Network-Network Interface |
| FCAPS | Fault management, Configuration management, Accounting management, Performance management, Security management |
| ID | Identifier |
| I-NNI | Internal Network-Network Interface |
| LRM | Link Resource Manager |
| 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 |
| SN | Subnetwork |
| SNP | Subnetwork Point |
| SNPP | Subnetwork Point Pool |
| TAP | Termination and Adaptation Performer |
| TMN | Telecommunication Management Network |
| TRI | Transport Resource Identifier |
| UNI | User Network Interface |
| VPN | Virtual Private Network |

# 5 Conventions

None.

# 6 Overview of control plane 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. 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, 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.

Before the network planning process starts, the operator should collect the traffic demands. These demands may come at different times. It is impossible to start the network planning process when each demand comes. So the demands are grouped, and the network planning process is periodically executed.

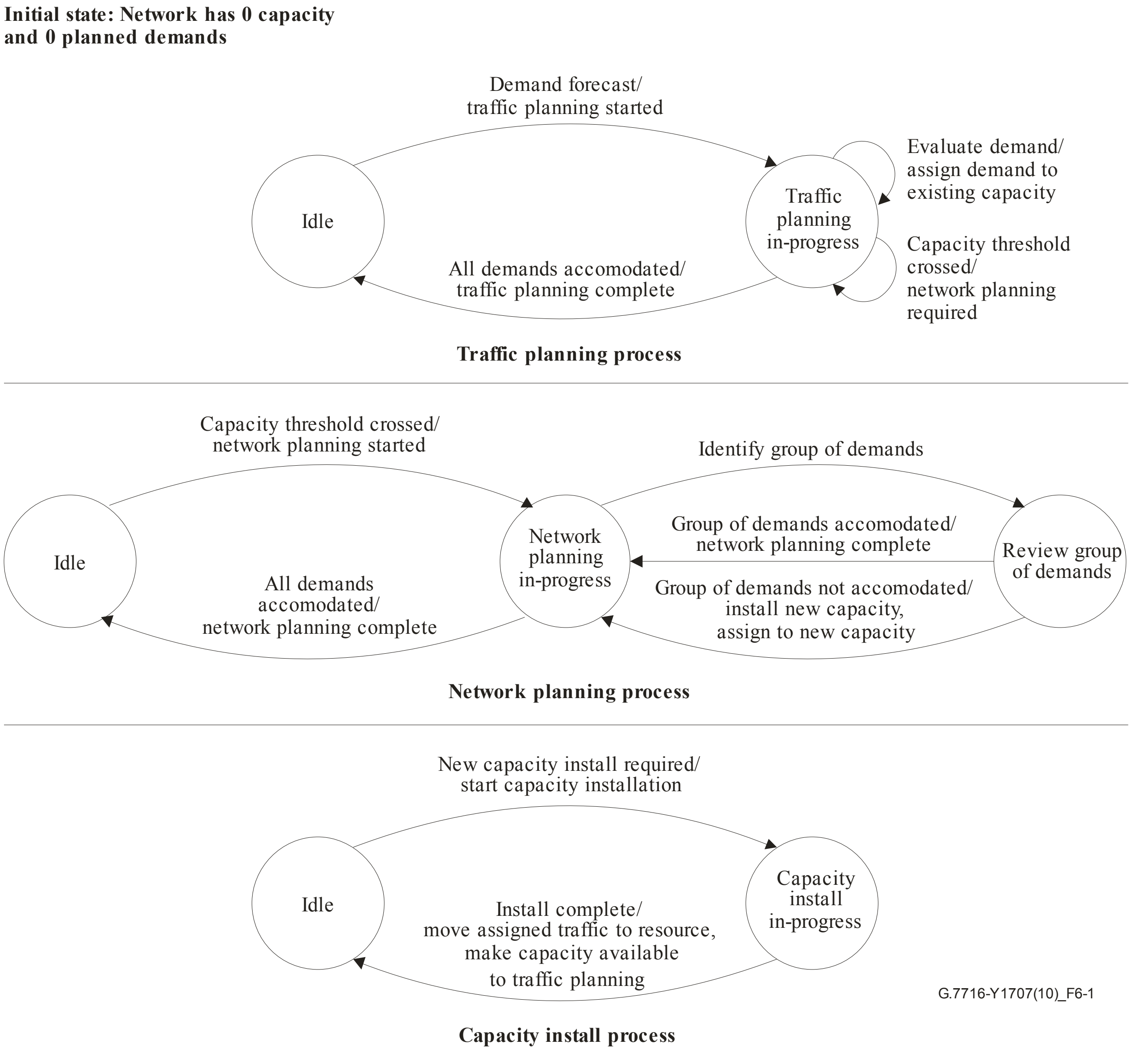


**Figure 6-1 – Three processes in transport network design and operation phases**

# 7 Automatically switched optical network plan

## 7.1 Transport network plan

As a part of the network engineering process, a transport network plan is developed and refined. This plan specifies the fundamental information needed to set up and operate an ASON. The information in the transport network plan can be divided into two categories: ASON Infrastructure and data plane topology. The necessary information for these two categories is shown in Table 7-1.

**Table 7-1 – Network structure plan information**

| ASON infrastructure | Data plane topology |
|---|---|
| • protocol selection<br>• control plane functional component distribution<br>• signalling network design<br>• component adjacency design | • subnetwork/routing area definition (Note 1)<br>• layer network relationships<br>• subnetwork/routing area hierarchy<br>• topology abstraction<br>• addressing structure (Note 2) |
| NOTE 1 – Subnetworks and routing areas are functionally identical, with some subtle differences. Clause 6.2 of [ITU-T G.8080] describes these differences.<br>NOTE 2 – These addresses are for the data plane and should not be confused with addresses in use in a signalling communication network (SCN). | |

Due to the dynamic nature of traffic forecasts, the transport network plan needs to be flexible – it must accommodate changes in network engineering. 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.

## 7.2 Management plane infrastructure

The management plane infrastructure for systems containing ASON functions is specified in [ITU-T G.7718] and [ITU-T G.7718.1]. [ITU-T G.7718] contains the framework for ASON management, putting ASON management within the telecommunication management network (TMN) context and specifying how the TMN principles may be applied. Requirements for ASON management information are specified so that a management information model can be developed.

[ITU-T G.7718.1] provides a protocol-neutral management information model for managing the ASON control plane. It identifies the TMN managed entities required. These entities are relevant to information exchanged across standardized interfaces defined in the Recommendation ITU-T M.3010 TMN architecture. The protocol-neutral management information model should be used as the base for defining protocol-specific management information models. The specific mapping of the protocol-neutral entities into protocol-specific managed object classes is the subject of the protocol-specific modelling design.

This Recommendation uses the ITU-T G.7718.1 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.

## 7.3 SCN 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 TMN, distributed signalling communications related to the ASON and other distributed communications. This Recommendation uses the ITU-T G.7712 architecture to describe the SCN available to control plane-enabled platforms and notes that the control plane components are dependent on that SCN infrastructure. Configuring and managing the SCN infrastructure is outside the scope of this Recommendation.

# 8 Initialization of control plane platforms

Initialization is the process of determining what resources exist, that they need to be bound to the appropriate control plane and management plane functional components, and that the control plane and management plane 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.

The actions performed when initializing an ASON control plane instance can be divided into four categories, as described in the following clauses.

## 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. 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.

Some configurations must be completed such as the node ID, area hierarchy, and so on, before the control plane starts up through initialization. The procedures of the local initialization include two steps: the control plane component activation and the control plane 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 Control plane component activation

The tasks and processes that support the functions described by the control plane 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 Control plane component binding configuration

The control plane components local to a platform or on peer platforms must coordinate with each other to fulfil the control plane functionality, so these control plane components must be bound to each other. This Recommendation discusses the binding required between platforms supporting control plane functions. The bindings internal to a platform are a matter for the implementation and out of scope of this Recommendation.

The relationship between control plane components is illustrated in Figures II.1 and III.1 of [ITU-T G.8080]. The bindings of the components need to be established at the initialization stage. These bindings may be software bindings or remote interface bindings. They may be static, provisioned or dynamic. Examples of bindings are NCC-CC, CC-RC, RC-LRM, as well as inter-layer NCC-NCC and inter-layer routing interaction, etc.

An SNPP is controlled by a specific CC, RC and 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.

An SNPP link is controlled by a CC-A and CC-Z as well as LRM-A and LRM-Z components. The bindings between CC-A and CC-Z as well as LRM-A and LRM-Z cannot be established until an SNPP link has 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.

The association between routing areas (RAs) (e.g., child RA and parent RA, local RA and remote 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. The information of the peer RC PCs (such as 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 maintained properly during routing initialization.

RC PCs are configured when a routing protocol is selected for an adjacency during routing initialization. Per [ITU-T G.8080], 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.7718.1] provides the specific attribute information required when creating an RC PC managed entity.

Per [ITU-T G.8080] 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 (UPN) 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.

### 8.2 Reconfiguration

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 control plane is different. During the commissioning state, the control plane components have not been placed into service yet. As a result, changes in the configuration of critical control plane components will not impact the set-up of new calls and connections as well as the continuation of existing calls and connections.

Some configurations during commissioning may be trial, so the operator needs to reconfigure some information according to the practical network environments for the control plane functions. For example, ASON control plane security functions should be tested, so encrypting OSPF-TE or RSVP-TE may be configured to examine the validity. However, according to current practical network environments, there is no need for control plane 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 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 control plane 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 control plane components and reported to the management plane. This notification would allow an operator to correct these errors before progressing to the operations and maintenance state.

## 9 Operation and maintenance

### 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. Resource changes may be the result of assigning an SNPP link to or removing an SNPP link from the control plane, 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 the property modification of a link that bears services must be made careful, because some properties of the link may be modified (e.g., the protection capability advertised for a link) but some properties of the link must not be modified (e.g., reducing the link protection provided by the transport plane below the protection level being advertised).

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

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

### 9.2 Resource assignment

A transport resource can be allocated to the management plane or control plane by the management plane or reserved by the management plane (it cannot be used to bear service even if it is configured by the management plane or control plane). If the transport resource is allocated to the management plane, the transport resource only can be available to the management plane. If the transport resource is allocated to the control plane, the control plane takes the role of "C" of FCAPS but the management plane can reallocate the transport resource to itself or as reserved resources. The change of resource allocation is allowed if service is not interrupted. The reserved transport resource cannot be used for services unless reallocated to the control plane or management plane.

The creation and deletion of control plane objects are defined in [ITU-T G.7718.1].

The management plane is responsible for maintaining the persistent store of configuration information required by the control plane, and the control plane should store the necessary configuration information persistently to avoid loss of configuration information when it is recovered from failure, etc.

### 9.3 Discovery/authentication process

The result of the discovery/authentication process can be utilized by the control plane for the link configuration process. The high-level process for accomplishing this is described in [ITU-T G.7714].

As the discovery process is performed, the information discovered should be validated by the control plane 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 control plane components or to verify the parameters configured by the management plane.

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

#### 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 management plane. 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.

### 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 plane 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 management plane configuration performed for adding a link.

#### 9.4.2 Authorization

Before adding a link to the control plane, 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 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 plane 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).

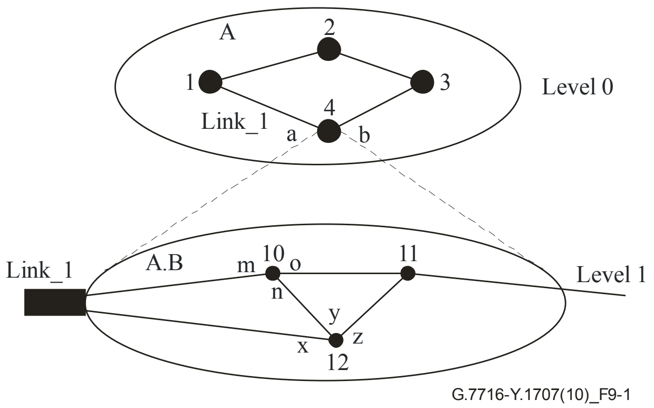


**Figure 9-1 – Example of SNPP alias use with abstract node**

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.

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}.

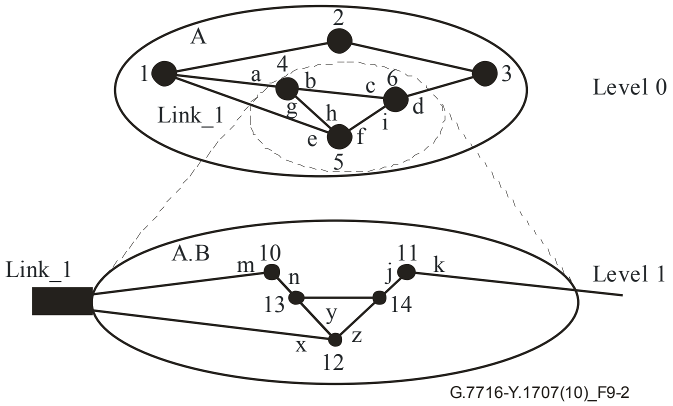


**Figure 9-2 – Example of SNPP alias use with abstract topology**

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.

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.8080] (topology and discovery).

#### 9.4.3.2 Use of alternate SNPP names for VPNs

See clause 6.3 of [ITU-T G.8080] (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 the remote end will provide its RC ID and RC PC SCN address to the local end.

### 9.6 Reconfiguration

Reconfiguration during the operations and maintenance state requires critical control plane components being taken out of service. This will impact the control plane'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 plane. The strategy required is specific to the type of reconfiguration being performed and the control plane 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 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. 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.

– Insertion of an RA into the hierarchy.

– Deletion of an RA from the hierarchy.

Though these reconfigurations may not be performed frequently, these reconfigurations will impact routing radically, so it should be more cautious before reconfiguration. In order to reduce the service impact for the routing oscillation, these reconfigurations should be performed according to careful plan in the least traffic time, such as midnight. If the reconfiguration impacts the policy boundary, then there is impact on signalling and traffic.

##### 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 example below shows the procedures of a single hierarchical level routing area splitting.

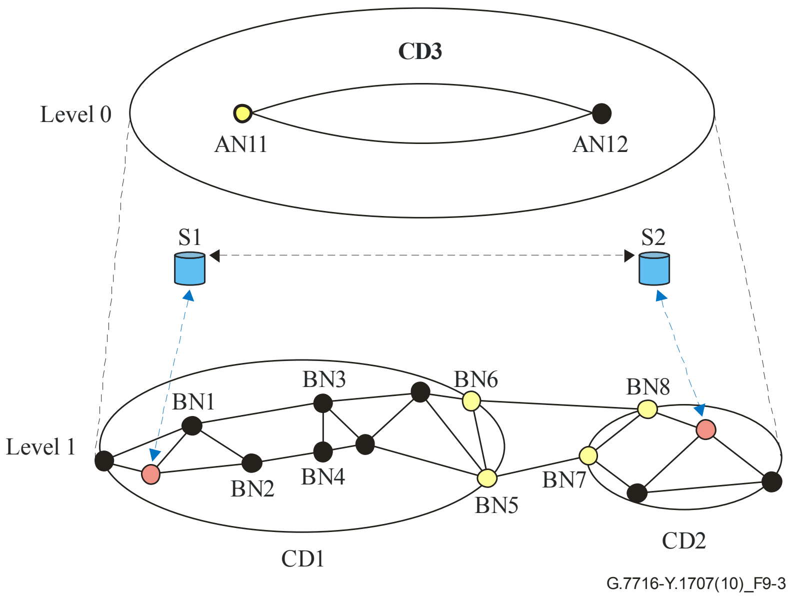


**Figure 9-3 – Initial topology**

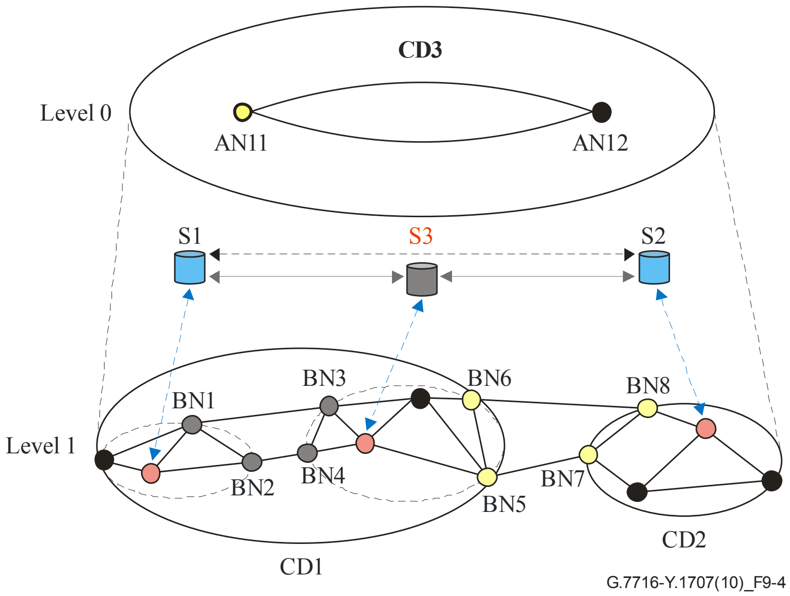


**Figure 9-4 – Intermediate status**

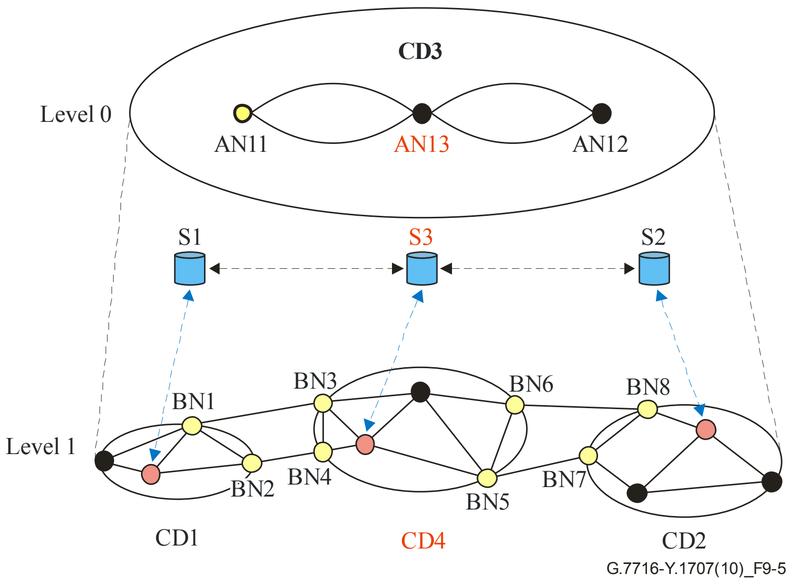


**Figure 9-5 – After splitting**

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 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.

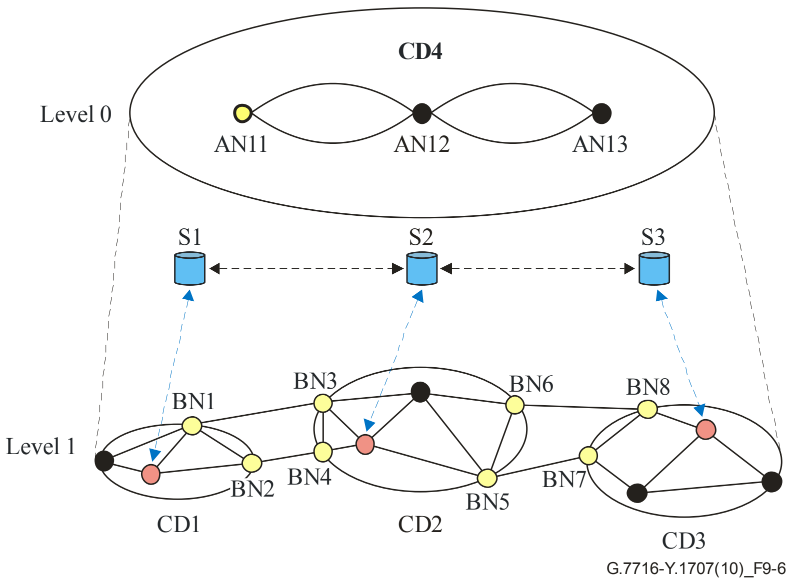


**Figure 9-6 – Initial topology**

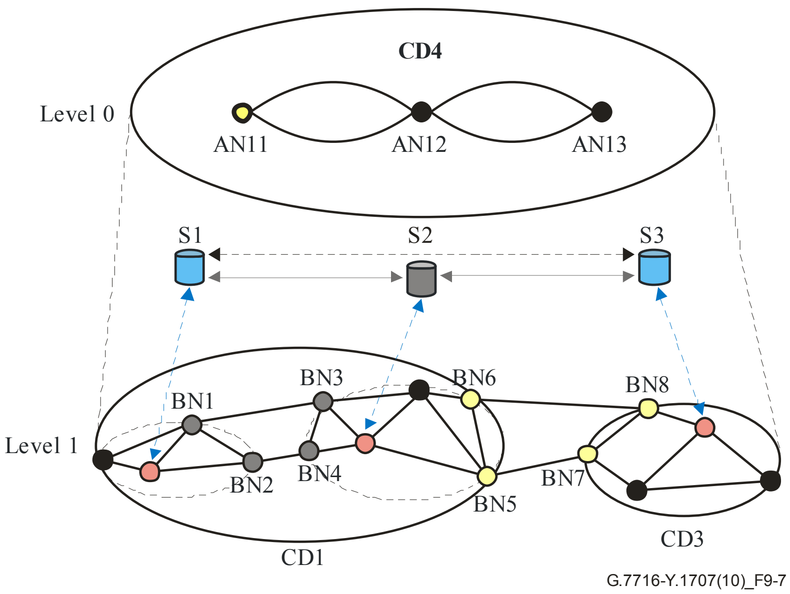


**Figure 9-7 – Intermediate status**

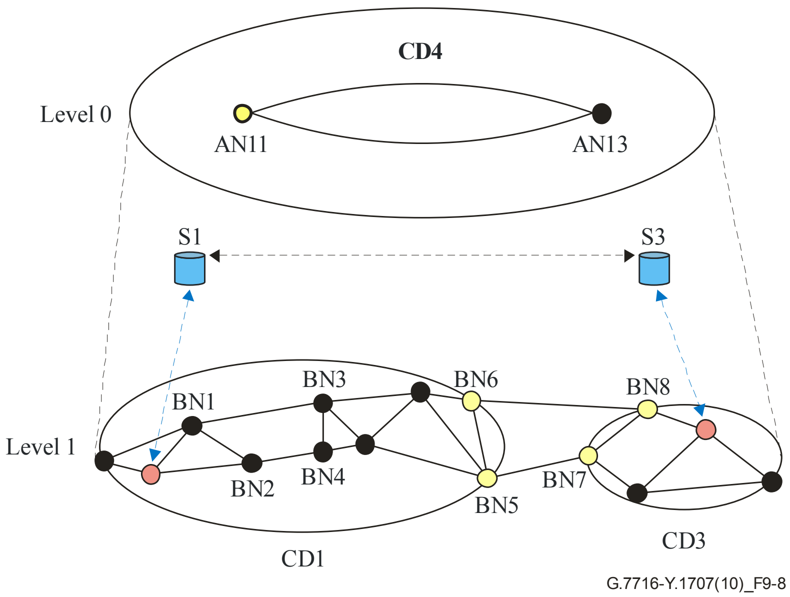


**Figure 9-8 – After merging**

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 be also be 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.

### 9.6.2.2 Routing area insertion/deletion

The general procedures of routing area insertion and deletion are described below.

#### 9.6.2.2.1 Routing area insertion

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

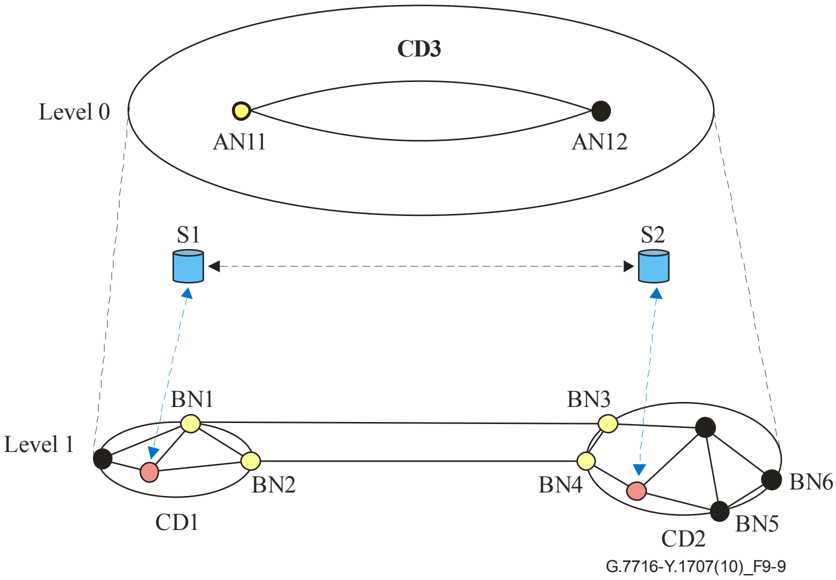


**Figure 9-9 – Initial topology**

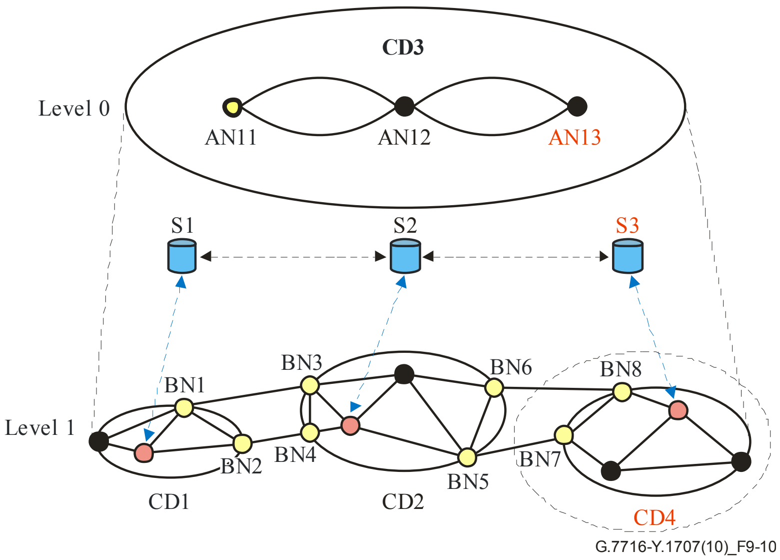


**Figure 9-10 – Routing area attachment**

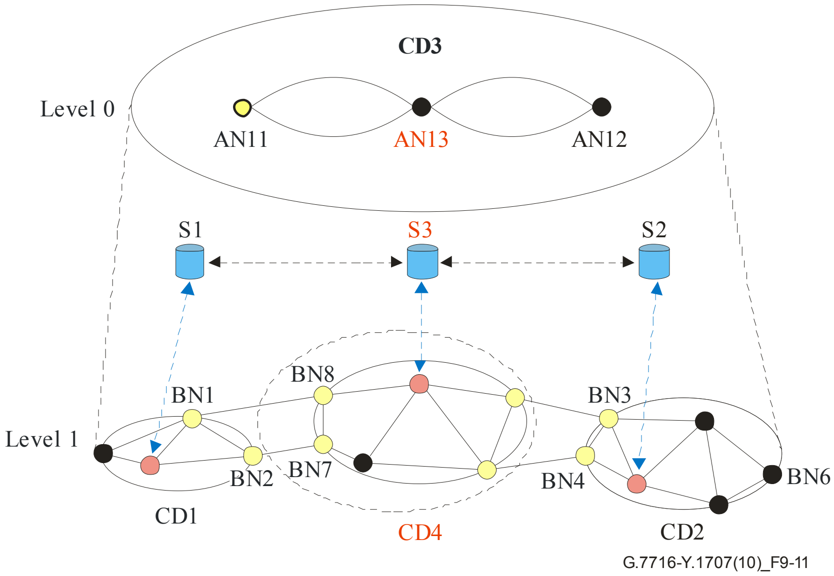


**Figure 9-11 – Routing area insertion**

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

1) Reconfigure AreaIDs of the inserting 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 inserted 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 insertion. 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 example below shows the procedures of a single hierarchical level routing area deletion.

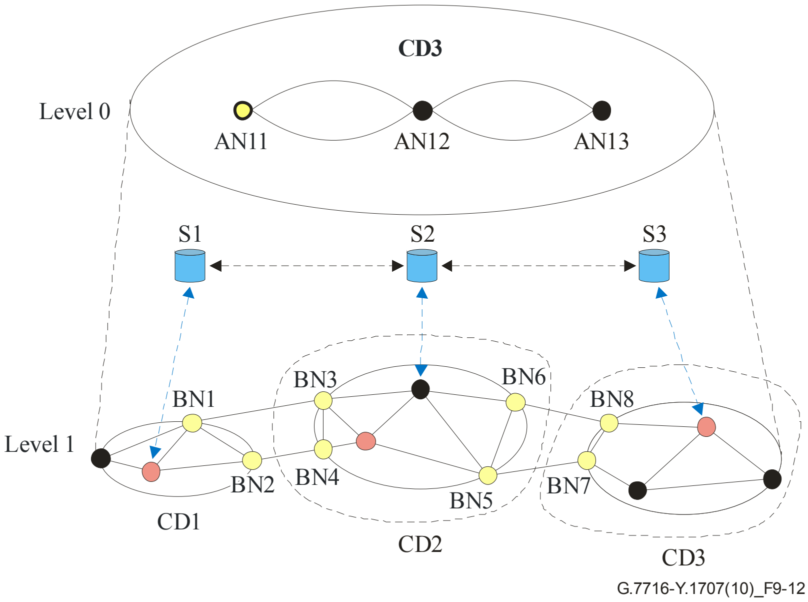


**Figure 9-12 – Initial topology**

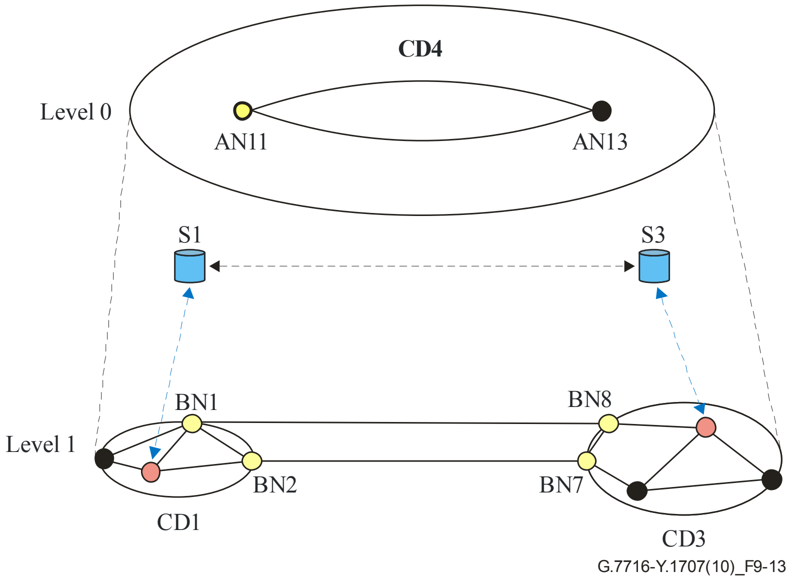


**Figure 9-13 – After deletion**

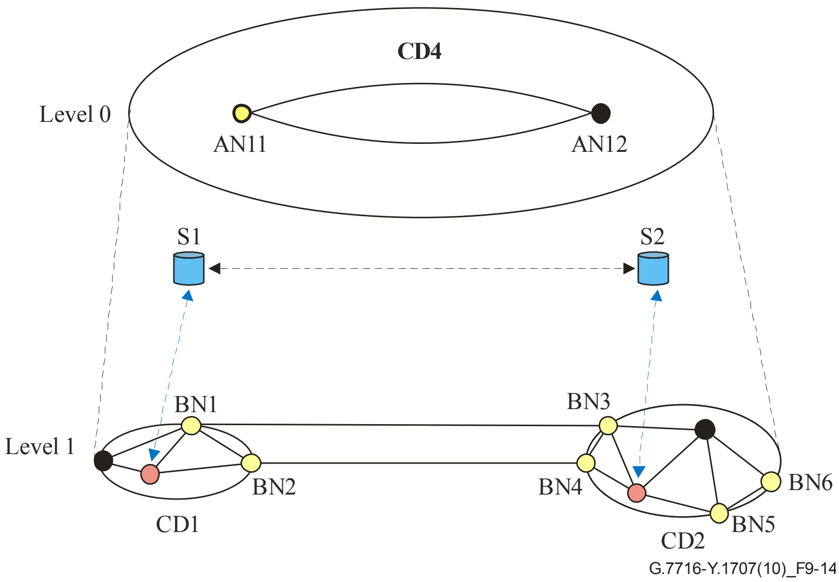


**Figure 9-14 – After deletion**

The procedures of 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.

## 9.7 Auditing

The auditing process is applied to the transport plane 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 plane resources between the control plane and the management plane within one node; it also includes checking the consistent views of the relevant transport plane resources between the control plane 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 plane and the transport plane.
– Inconsistency between control plane peers is detected.
– Inconsistency between control plane and transport plane is detected.

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 control plane/transport plane

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

#### 9.7.1.1 Resource state

When an SNP is assigned by the management plane to the control plane, the control plane 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 plane action.

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

The interface that provides this indication is for further study.

### 9.7.2 Between control plane peers

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

#### 9.7.2.1 SNP state

When a transport plane CP link connection is allocated to support the control plane 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 plane CP link connection can be allocated to support the control plane SNP link connection. If any inconsistency is detected for resources that have been assigned to the control plane, the control plane should report to the management plane.

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 management plane and control plane 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 management plane and control plane 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 management plane. 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 management plane 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 management plane can be modified by the management plane and the control plane 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 management plane 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 control plane should report success to the management plane. If there is any mismatch in the consistency check, corresponding alarm information should be reported to the management plane 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 management plane, users can reconfigure the link attribute and then to trigger the control plane 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 plane, various fault conditions might occur. The ASON architecture described in clause 12 of [ITU-T G.8080] provides guidance for recovery of the control plane from these conditions.

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

A vertical consistency check is performed between the control plane, transport plane and management plane. A horizontal consistency check is performed between local and remote control plane 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.

# Appendix I

## Initialization example

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

The start-up sequence of the control plane components is based on the components' dependency relationships, so the depended components should be initialized prior to the depending components. The binding of the control plane 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 plane initialization is illustrated in Figure I.1:

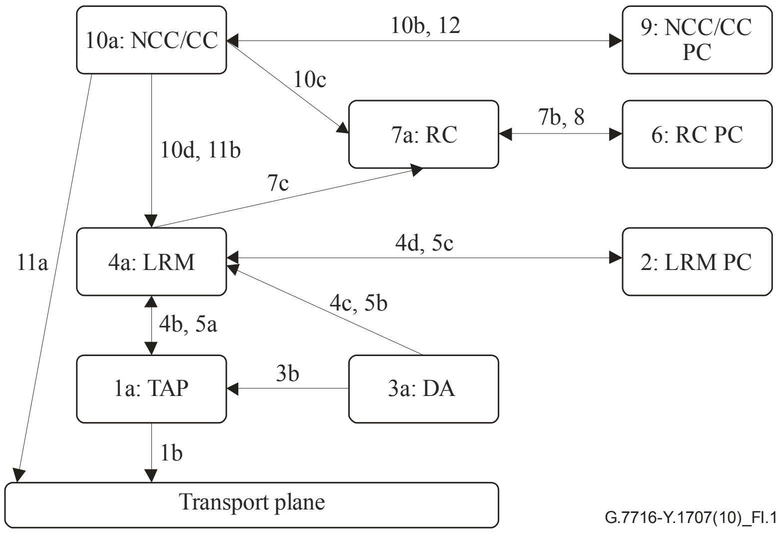


**Figure I.1 – Control plane initialization process**

1) Starts TAP component. It gets connection point (CP) information (e.g., CP name, signal type, bandwidth and CP status) from transport plane. Then TAP will be informed of CP-SNP relationship.
2) Starts 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) Starts DA component. It associates itself with TAP component and discovers CP link connections within the transport name space.
4) Starts 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) Starts signalling PC component. It gets RC ID and signalling PC SCN address information from permanent storage to establish their binding relationship.
7) Starts 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) RC component communicates with peer RC components to synchronize network topology information.

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

10) Starts 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 plane and transport plane 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 management plane to take further action.

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS**

| | |
|---|---|
| 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 |
| 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 |
| Numbering, naming and addressing | Y.2300–Y.2399 |
| Network management | Y.2400–Y.2499 |
| Network control architectures and protocols | Y.2500–Y.2599 |
| Security | Y.2700–Y.2799 |
| Generalized mobility | Y.2800–Y.2899 |

*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 | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| **Series G** | **Transmission systems and media, digital systems and networks** |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | 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 |
| 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 and next-generation networks** |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2010