International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3712

(08/2016)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for SDN – Resource control protocols

Scenarios and signalling requirements of unified intelligent programmable interface for IPv6

Recommendation ITU-T Q.3712

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
Resource control protocols	**Q.3710–Q.3739**
TESTING SPECIFICATIONS	Q.3900–Q.4099

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

Recommendation ITU-T Q.3712

Scenarios and signalling requirements of unified intelligent programmable interface for IPv6

Summary

Recommendation ITU-T Q.3712 describes the scenarios and signalling requirements of unified intelligent programmable interface for IPv6 service deployment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3712	2016-08-29	11	11.1002/1000/12990

Keywords

IPv6, SDN, transition.

* 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, 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/.

Table of Contents

Recommendation ITU-T Q.3712

Scenarios and signalling requirements of unified intelligent programmable interface for IPv6

1 Scope

This Recommendation describes the scenarios and signalling requirements of unified intelligent programmable interface for IPv6 service deployment. The example signalling protocol procedures at this interface will also be described in this Recommendation to support protocol unaware flow forwarding in the data plane. The IPv6 technologies supported in this Recommendation will include, but not be limited to, the following: dual-stack lite (DS-Lite), IPv6 only, IPv6 rapid deployment (6rd), IPv4 residual deployment (4rd), mapping of address and port - encapsulation mode (MAP-E), mapping of address and port - translation mode (MAP-T), lightweight 4over6 (lw4over6) and 464XLAT.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 software-defined networking [b-ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ALG	Application Level Gateway
App	Application
DS-Lite	Dual-Stack Lite
lw4over6	Lightweight 4over6
NAT64	Network Address Translation 64
NETCONF	Network configuration protocol
RG	Residential Gateway
SDN	Software-Defined Networking
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
4rd	IPv4 Residual Deployment
6rd	IPv4 Rapid Deployment

5 Conventions

None.

6 The deployment scenario and use cases

6.1 Evolve from one IPv6 transition scenario to another

During the IPv6 transition period, the network has three types: IPv4-only, dual-stack and IPv6-only. The networks should support both IPv4 services and IPv6 services at each stage. There are multiple IPv6 transition technologies for different network scenarios (e.g., IPv4 network for IPv4/IPv6 user access, IPv6 network for IPv4/IPv6 user access, IPv4 servers for IPv6 visitors). Different network scenarios will co-exist during IPv6 transition which means the IPv6 transition device should support multiple IPv6 transition technologies. The following are six possible scenarios of IPv6 transition:

1) IPv6 host visits IPv6 servers via IPv4 access network;
2) IPv4 host visits IPv4 servers via IPv4 NAT dual-stack network;
3) IPv6 host visit IPv6 servers via IPv6 network;
4) IPv4 host visits IPv4 servers via IPv6 access network;
5) IPv6 host visits IPv6 servers via IPv4 access network;
6) IPv4 host and IPv6 host interaction.

It is not necessary that every operator goes through each scenario one by one. For example, some operators may start from scenario 1), and some may start directly from scenario 2) or scenario 4). However, since the final stage (target) is an IPv6-only access network, one still needs to go through multiple scenarios from a long-term perspective.

In such a case, the operator should either upgrade existing devices to support new features, or replace them with new ones. In particular, when the operator's network consists of devices from different vendors, it is hard to guarantee that all legacy devices can be upgraded at the same time. This is costly and complicated.

6.2 Multiple transition mechanisms co-exist

Currently, there are multiple transition mechanisms in the industry, e.g., DS-Lite, lw4over6, mapping of address and port (MAP)/4rd, network address translation 64 (NAT64). In the transition from one scenario to another, different mechanisms may have different impacts on user experience. For example, DS-Lite would have some impact due to address sharing as compared with 6rd mechanisms, and NAT64 would have an additional impact due to application level gateway (ALG) issues. Operators need to offer a fallback mechanism to guarantee the same level of user experience when there are complaints from subscribers. Therefore, it is required to support multiple transition mechanisms in the same area (even in the same device).

Another use case is that multiple scenarios may exist in the same stage. For example, if both IPv6-only devices and IPv4-only hosts are in the same area with limited public IPv4 address, then NAT64 and NAT44 (or DS-Lite) are both required to achieve IPv4 service connectivity.

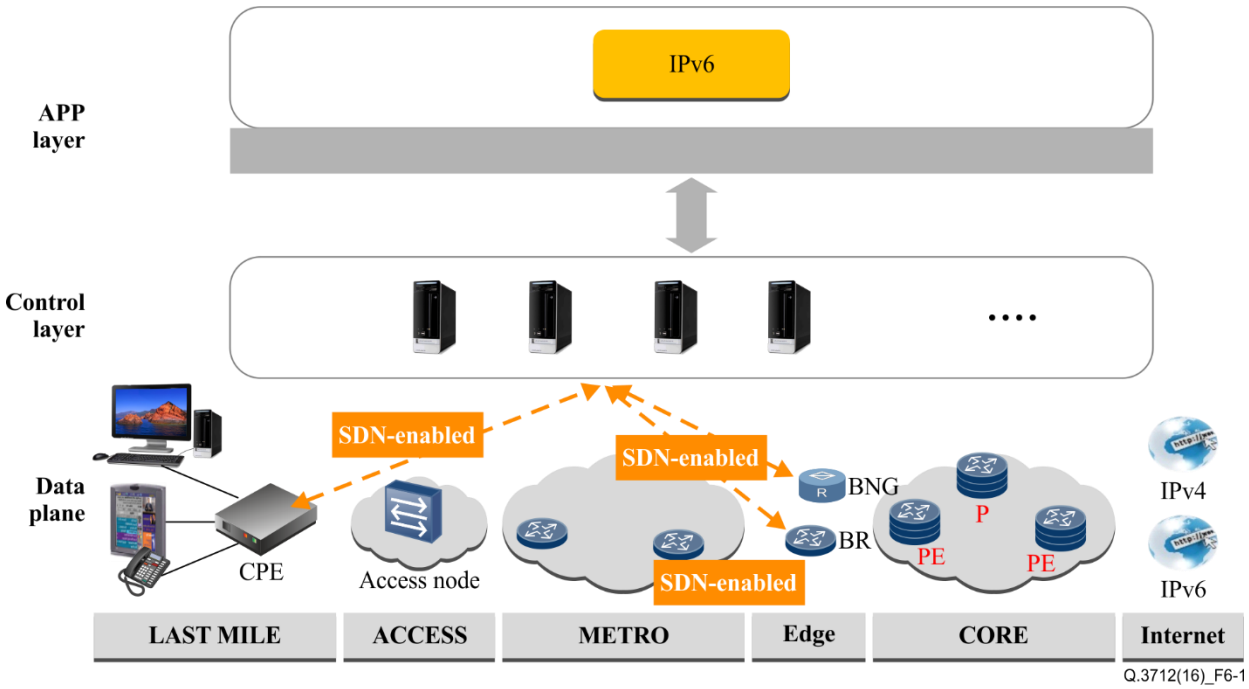

Figure 6-1 – Scenario and use case of this Recommendation

The unified intelligent IPv6 deployment scenario offers end-to-end service deployment and management. The residential gateway (RG), the IP edge and the service edge are flow-forwarding enabled. The hardware can be unified for different IPv6 transition technologies via flow-forwarding. IPv6 transition technologies can be plugged into the controllers. The flow-forwarding enabled devices do not need to change during the various stages of IPv6 transition.

The northbound interface is essential to support the eco-system of software-defined networking (SDN) by allowing various SDN-related applications to be plugged in various vendor controllers. The goal is to make the controller controlled infrastructure to be an open platform for more innovations by allowing applications to be developed with the best network support.

Several OpenFlow switches are deployed and located at the edge of network, as shown in Figure 6-1. The OpenFlow protocol may be extended mainly to support an IP tunnelling approach for transition purposes. The OpenFlow switches process the incoming packets based on the flow tables delivered by the SDN controller upon the request of an IPv6-transition application (App).

The controller in the control layer provides an interface to the IPv6 transition App, enabling it to modify traffic processing using OpenFlow. Specifically, the controller provides an OpenFlow driver that enables the IPv6 transition App to instruct all SDN-enabled device how to treat traffic, thus making it possible to flexibly choose the particular transition mechanism to be applied, and to select the parameters governing it. The OpenFlow driver includes OpenFlow protocol specific tasks: listens for OpenFlow connections, creates the channel, keeps alive, proxy between the OpenFlow wire format and the solution internal information representation (e.g., rules, events). It is a basic function of the SDN controller.

The process shown for this case is generic. A flow can be identified by part of the layer 2 (L2) to layer 4 (L4) packet header information. For example, all packets to a particular subscriber can be treated as belonging to the same flow in an SDN-enabled network.

SDN provides a programmable platform for service deployment which can reduce new issues arising in the IPv6 transition.

7 The signalling architecture

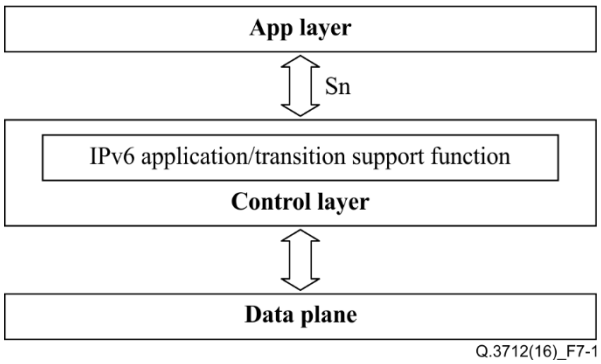

Figure 7-1 – Signalling interface

IPv6 transition technologies are presented as software Apps and are loaded into the control layer which is responsible for IPv6 application/transition support function via plug-in method. An IPv6 application/transition support function interface (Sn), which may use network configuration protocol (NETCONF)/YANG, describes IPv6 application/transition support function needed, which is independent of IPv6 application/transition technologies. The App layer generates the operation request based on the IPv6 application/transition support function data model configured, and sends the request to the IPv6 application/transition support function in the control layer. The IPv6 application/transition support function enables the Apps to manipulate the traffic via the Sn interface.

8 Signalling requirements

8.1 Component functions

8.1.1 App layer

The application modules in the App layer provide the abstracted application program interfaces (APIs) and/or user functions. It receives the packet about the IPv6 transition technologies APP of new IPv6 flows from the control layer after the control layer receives the events from the network devices in the data plane. Then it sends appropriate instructions to the SDN-enabled device via the control layer and the Sn interface.

8.1.2 Control layer

The control layer provides a northbound interface (Sn) that enables the IPv6 transition technologies App to modify the traffic using OpenFlow. It receives the events from the network devices and sends it to the App layer if necessary. After receiving the instructions from the App layer, the control layer translates the commands of the IPv6 transition technologies APP to a command that can be executed by the SDN-enabled device.

8.2 Interface requirements

The control layer provides a northbound interface (Sn) that enables the IPv6-transition App to modify traffic at the data plane using OpenFlow. Specifically, the control layer provides an OpenFlow driver that enables the IPv6-transition App to decide how the SDN-enabled packet-forwarding devices treat traffic using the Sn interface. This interface is used to provide an IPv6 application/transition support function interface to any IPv6-transition application. It mainly provides the following functions:

– Registration and removal function for applications;

– IPv6 application/transition support function data model for packets and flow tables interaction between controller and applications;

– Adapting packet-in events into neutral events in the interface;
– Supporting the installation function for applications in the interface. The control layer enables the application to program the data plane. The App layer determines the technology to be used and sets the parameters for it;
– The Sn interface should distribute the up-called events to the appropriate App functions based on the registered features of the App functions;
– Providing the management functions for the App functions to configure and manage the installed modules in the controller.

The control layer provides a mechanism for new services/applications creation and existing services/applications removal via the Sn interface. A specified transmission control protocol (TCP) port number is provided for application registration, removal and coordination. When a new application is needed in the unified IPv6 system, this new application will initiate a registration request to the control layer using the specified TCP port number. Then the application and the control layer will coordinate an App ID and a dedicated channel for this App. Then the new App will register its features (e.g., the appropriate packet type(s) handled by the App) and/or install some function(s) to the control layer via the dedicated channel of the App. Removal function is also achieved via the specified TCP port number.

8.2.1 Flow description

In this Recommendation, two parts of the flow table for IPv6 transition technology will be defined: Match fields and Actions.

Match Fields	Actions

The procedure to create the flow table is separated into two steps:

1. The Match field is defined as below:

Field Offset	
Field length	

2. The possible Actions of the Protocol-Unaware flow table are defined as: Action Type, e.g., set-field, add-field and del-field.

   Taking the set-field and add-field as examples:

Action Type	**Set-field**
Set-field offset	
Set-field length	

Action Type	Add-field
Add-field offset	
Add-field length	

8.2.2 IPv6 transition parameters in the flow table

The Sn interface enables the IPv6/IPv6 transition technology applications to manipulate traffic. The parameters appearing in the flow table may be transmitted at this interface, which contains the following information:

– tunnel_sip_v6: The source ipv6 address of tunnel (if any);
– tunnel_dip_v6: The destination ipv6 address of tunnel (if any);
– tunnel_sip_v4: The source ipv4 address of tunnel (if any);
– tunnel_dip_v4: The destination ipv4 address of tunnel (if any);
– sip_v6: The source ipv6 address of a packet or inner source ipv6 address when packet type is IP-in-IP tunnel;
– dip_v6: The destination ipv6 address of a packet or inner destination ipv6 address when packet type is IP-in-IP tunnel;
– sip_v4: The source ipv4 address of a packet or inner source ipv4 address when packet type is IP-in-IP tunnel;
– dip_v4: The destination ipv4 address of a packet or inner destination ipv4 address when packet type is IP-in-IP tunnel;
– sip_v6_port: Source IPv6 TCP/user datagram protocol (UDP) port number of the source ipv6 packet (or inner source ipv6 packet when packet type is IP-in-IP tunnel);
– dip_v6_port: Destination IPv6 TCP/UDP port number of the destination ipv6 packet (or inner destination ipv6 packet when packet type is IP-in-IP tunnel);
– src-port: source TCP/UDP port number of a packet;
– dst-port: Destination TCP/UDP port number of a packet;
– set_ip/port: Modify the IP or/and port number in the header of the packet.

9 The signalling protocol procedures

The flow in this use case is generic. A flow can be identified by part of the L2-to-L4 packet header information (e.g., all packets to a subscriber can be considered to belong to the same flow in the SDN-enabled device, which will greatly reduce the number of flows). The signalling procedures, as illustrated in Figure 9-1, are as follows:

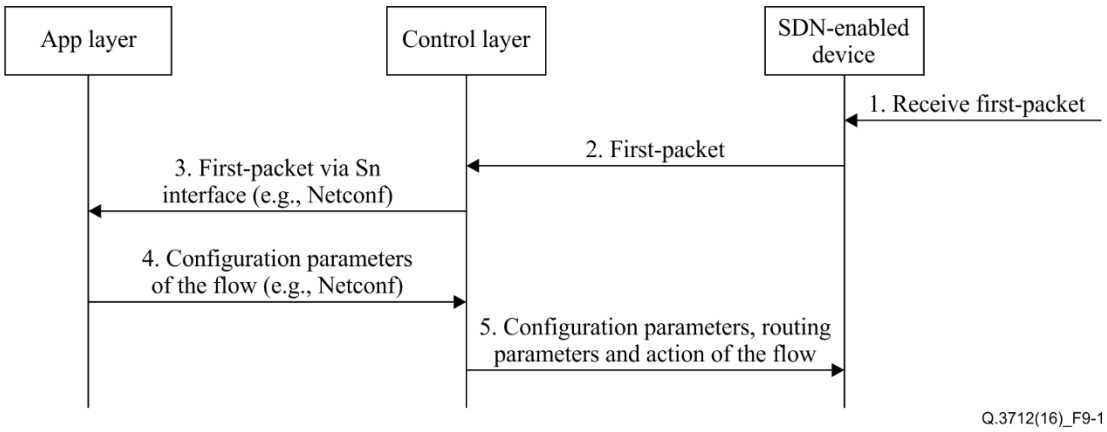

Figure 9-1 – Signalling procedures of this Recommendation

1. Receiving a first-packet of a flow at the SDN-enabled device;
2. The first-packet is sent to the control layer from the SDN-enabled device, and the open flow protocol may be used at this interface;
3. The first-packet is sent to the APP layer via the Sn interface, and NETCONF may be used;
4. The configuration parameters (e.g., flow table) of the flow are sent out from the App layer to the control layer via the Sn interface. The parameters transmitted are shown in clause 8.2.2;
5. The configuration parameters, routing parameters and corresponding actions of the flow are sent out from the control layer to SDN-enabled device. The SDN-enabled device will add the new flow to the flow table.

The subsequent packets of the flow received by the SDN-enabled device will then be processed based on the flow table, causing the SDN-enabled device to forward tunnelled IPv6 packets to their proper destination. Some method can be achieved to improve the SDN efficiency. Permanent (rather than per-flow) or even pre-configured flows could be achieved as well.

9.1 Information model

Information model matches the OpenFlow protocol specification and is slightly extended to support IP-in-IP tunnels. It can accommodate multiple switches (using the datapath id to identify switches or using the IP address of the datapath).

The data structure is specified as

– tunnel_sip_v6: The src-ipv6 address of tunnel (if any);
– tunnel_dip_v6: The dst-ipv6 address of tunnel (if any);
– tunnel_sip_v4: The src-ipv4 address of tunnel (if any);
– tunnel_dip_v4: The dst-ipv4 address of tunnel (if any);
– sip_v6: The src-ipv6 address of a packet or inner src-ipv6 address when packet type is IP-in-IP tunnel;
– dip_v6: The dst-ipv6 address of a packet or inner dst-ipv6 address when packet type is IP-in-IP tunnel;
– sip_v4: The src-ipv4 address of a packet or inner src-ipv4 address when packet type is IP-in-IP tunnel;
– dip_v4: The dst-ipv4 address of a packet or inner dst-ipv4 address when packet type is IP-in-IP tunnel;
– sip_v6_port: Source IPv6 TCP/UDP port number of the src-ipv6 packet (or inner src-ipv6 packet when packet type is IP-in-IP tunnel);

– dip_v6_port: Destination IPv6 TCP/UDP port number of the dst-ipv6 packet (or inner dst-ipv6 packet when packet type is IP-in-IP tunnel);
– src-port: Source TCP/UDP port number of a packet;
– dst-port: Destination TCP/UDP port number of a packet.

9.2 Operations

The supported operations match the OpenFlow operations (packet out, flow mod, and all the others) are extended with IP-in-IP support, as follows:

– push_ipv4_header: Encapsulate the packet into an IP-in-IP tunnel, tunnel type is IPv4;
– pop_ipv4_header: De-capsulate the packet from IP-in-IP tunnel, tunnel type is IPv4;
– push_ipv6_header: Encapsulate the packet into an IP-in-IP tunnel, tunnel type is IPv6;
– pop_ipv6_header: De-capsulate the packet from IP-in-IP tunnel, tunnel type is IPv6.

Appendix I

Protocol profiles for this Recommendation

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

The NETCONF [b-IETF RFC 6241] is a candidate configuration protocol for the interface between the App layer and the control layer to facilitate the description of the IPv6 application/transition support function and the generation of the operation request (e.g., set, add and delete), further to enable the Apps to manipulate the traffic via the Sn interface.

This Recommendation requires that the NETCONF "Capabilities Exchange" capability be supported. The following protocol operations should also be supported:

– <get>
– <get-config>
– <edit-config>
– <copy-config>
– <delete-config>

Bibliography

[b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[b-IETF RFC 6241] IETF RFC 6241 (2011), *Network Configuration Protocol (NETCONF)*.

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	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	Terminals and subjective and objective assessment methods
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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016