International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2621

(08/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Smart ubiquitous networks

Requirements for an independent, scalable control plane in future, packet-based networks

Recommendation ITU-T Y.2621

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
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
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous 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.3099

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

Recommendation ITU-T Y.2621

Requirements for an independent, scalable control plane in future, packet-based networks

Summary

Recommendation ITU-T Y.2621 describes the technical requirements for an independent, scalable control plane (iSCP) by separating the control plane from the data plane in future packet-based networks (FPBNs). The requirements include reachability, scalability, flexibility, reliability, manageability, service, security, interworking, routing and forwarding.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2621	2011-08-06	13

Keywords

Forwarding, FPBN, iSCP, network entity, routing, scalability, separation, virtual network element.

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

Page

Introduction

The rapid, continued increase of the number of users, their bandwidth and service requirements, the scalability and controllability of the control plane, the data plane and the management plane of network nodes and of the whole network, are major challenges for future evolution. One of the reasons for issues related to the scalability and controllability of today's IP networks is that the functional architecture of the control plane is not optimal. In current IP networks, the control plane and the data plane are integrated into network nodes, and more and more control and service functionalities are added in the network nodes. IP networks have become complex, thus making it difficult to maintain or extend them.

The independent, scalable control plane (iSCP), which separates the control plane from the data plane in future packet-based networks (FPBNs), can alleviate such problems of scalability and controllability in current IP networks. The iSCP has specific requirements derived from its architectural characteristics.

Recommendation ITU-T Y.2621

Requirements for an independent, scalable control plane in future, packet-based networks

1 Scope

This Recommendation describes the technical requirements for an independent, scalable control plane (iSCP) by separating the control plane from the data plane in future packet-based networks (FPBNs) as described in [ITU-T Y.2601]. Recognizing scenarios described in [b-ITU-T Y-Sup. 11], the requirements of iSCP provided in this Recommendation cover reachability, scalability, flexibility, reliability, manageability, services, security, interworking, routing and forwarding.

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 Y.2011]	Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*
[ITU-T Y.2601]	Recommendation ITU-T Y.2601 (2006), *Fundamental characteristics and requirements of future packet based networks.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control plane [ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.

3.1.2 data plane [ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.3 management plane [ITU-T Y.2011]: The set of functions used to manage entities in the stratum or layer under consideration, plus the functions required to support this management.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 future packet-based network (FPBN): A network architecture providing the topmost layer(s) of the transport stratum as defined in [ITU-T Y.2011].

NOTE 1 – This definition is based on the description of FPBN in [ITU-T Y.2601].

NOTE 2 – Fundamental characteristics and requirements of future packet-based networks are defined in [ITU-T Y.2601].

3.2.2 independent scalable control plane (iSCP): An architectural approach of future packet-based networks (FPBNs) which consists in separating the control plane from the data plane.

NOTE – Fundamental characteristics and requirements of future packet-based networks are defined in [ITU-T Y.2601].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CE	Control Element
FE	Forwarding Element
FIB	Forwarding Information Base
FPBN	Future Packet-Based Network
iSCP	independent, Scalable Control Plane
LSP	Label Switched Path
ME	Management Element
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
P2P	Peer-to-Peer
QoS	Quality of Service
RIB	Routing Information Base
SCE	Service Control Element
SPE	Service Processing Element
TTL	Time To Live
VNE	Virtual Network Element
VPN	Virtual Private Network

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement needs not to be present to claim conformance.

The keyword "entity" indicates a CE, SCE, FE, SPE, ME or VNE.

6 Overview of iSCP

As shown in Figure 6-1, iSCP adopts a particular architecture that separates the control plane from the data plane in the future packet-based network (FPBN).

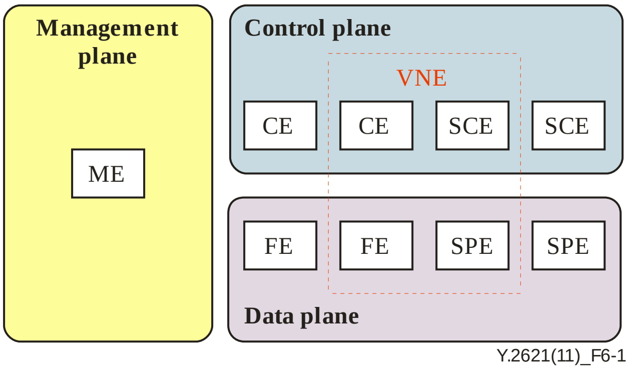

Figure 6-1 – Overview of iSCP

The control plane of iSCP contains mechanisms dealing with operating the packets and deciding the pathways for user traffic. These mechanisms will be implemented in control elements (CEs) and service control elements (SCEs). The data plane of iSCP contains mechanisms for forwarding and processing user traffic. These mechanisms will be implemented in forwarding elements (FEs) and service-processing elements (SPEs). The management plane of iSCP contains mechanisms dealing with the operation, administration and management aspects of an iSCP-based network, which is a network based on iSCP as an architectural approach. These mechanisms will be implemented in management elements (MEs).

In the context of iSCP, a single conventional network entity, e.g., a router, can be constructed using multiple network entities such as CEs, SCEs, FEs and SPEs. The resulting constructed entity is called a virtual-network element (VNE). Depending on the required capacity and flexibility, the number of individual entities used for the VNE can vary. In a typical scenario, a small number (e.g., one or two in a case of redundancy) of CEs control a large number of FEs.

In a VNE, one CE can control one or a group of FE(s) through the control plane. The CE will generate the rules for FE(s) to forward certain traffic, and download the rules to FE(s). To generate these rules, the CE maintains necessary information in a routing information base (RIB) to compute the most suitable route for incoming packets. The RIB is updated by communicating with other CEs through routing protocols. Then CE(s) generate a forwarding-information base (FIB) based on the RIB, and download the FIB to FE(s).

One SCE can control associated SPE(s) through the control plane. The SCE maintains a policy database and generates the rules for SPE(s) to process certain traffic. These rules are based on service policies, configured by ME(s), and are maintained as a service-control table. For example, service policies include QoS behaviour policies and access-control policies. The SCE enforces the rules by setting service control table(s) in the associated SPE(s).

An FE forwards incoming packets according to the FIB that was generated and given through the control plane by the CE(s). The FE receives and updates the FIB from the CE, looks up the FIB to obtain the next-hop information of packets, and forwards the packets.

An SPE handles incoming packets according to the service control table. The SPE receives and updates the service control table given through the control plane by the SCE(s), looks up the table, and handles packets according to the table. The SPE can process packets with some mechanisms such as network-address translation (NAT), encryption/decryption, protocol conversion, content processing, etc.

An ME manages the resources of CE(s), SCE(s), FE(s) and SPE(s) in terms of configuration, fault, accounting, performance, and security management, through the management plane.

7 iSCP requirements

This clause describes the requirements derived from the characteristics of iSCP as described in clause 6. These requirements cover: reachability, scalability, flexibility, reliability, manageability, services, security, interworking, routing and forwarding.

7.1 Reachability

(1) The iSCP is required to support communication mechanisms between CEs and FEs and between SCEs and SPEs.

(2) The iSCP is required to support the route checking mechanisms to confirm the reachability between CEs and FEs and between SCEs and SPEs.

7.2 Scalability

(1) The iSCP is required to support scalability of the capacities, performance and functions of CEs, FEs, SCEs and SPEs, independently.

(2) The CE is required to control multiple FEs. The number of FEs controlled by one CE is required to be changed easily in the iSCP-based network.

(3) The SCE is required to control multiple SPEs. The number of SPEs controlled by one SCE is required to be changed easily in the iSCP-based network.

(4) The iSCP is required to support scalable sizes of the RIB in the CE, of the policy database in the SCE, of the FIB in the FE, and of the service-control table in the SPE.

7.3 Flexibility

(1) The iSCP is required to provide easy and flexible addition, deletion, and upgrading of the functions supported by CEs, FEs, SCEs and SPEs.

(2) The iSCP is required to provide easy and flexible addition, deletion, and upgrade of CEs, FEs, SCEs and SPEs in the iSCP-based network.

(3) The iSCP is required to cope with frequent topology changes, such as adding, deleting and changing the status of CEs, FEs, SCEs and SPEs.

7.4 Reliability

(1) The iSCP is required to support mechanisms for fault tolerance of CEs and SCEs. Backup CEs and SCEs are recommended to be provided.

(2) The iSCP is required to enable CEs, FEs, SCEs and SPEs to detect faults of their connected entities, to restore the connections with the recovered or alternate entities, and to (re)synchronize the status.

(3) The iSCP is required to allow multiple CEs and SCEs to work together to support load-balancing for different application scenarios.

7.5 Manageability

(1) The iSCP is required to allow ME(s) to manage all entities resources. This includes the means of accessing all entities in a distributed environment and the capabilities of monitoring and configuring all entities resources.

(2) The iSCP is required to allow ME(s) to deliver the configuration information for constructing a given VNE to the entities that will constitute that VNE, so that these entities be able to construct this VNE based on the required configuration.

(3) The iSCP is required to allow ME(s) to manage management information bases (MIBs) of all entities, including CEs, FEs, SCEs, SPEs and VNEs.

7.6 Services

(1) The iSCP-based network is required to support the transport functions required for the support of NGN services and Internet services.

(2) The iSCP-based network is required to support tunnelling functions, such as for the support of MPLS LSP tunnels, etc.

(3) The iSCP-based network is required to support VPN functions, such as related to MPLS VPN, etc.

7.7 Security

(1) The iSCP is required to protect the communication between entities from attacks, such as man-in-the-middle, snooping and impersonation.

(2) The iSCP is required to support service-traffic isolation among multiple services (see clause 7.6 (1)).

7.8 Interworking

(1) The iSCP-based network is required to communicate with legacy networks, such as IP- or MPLS-based networks, by edge equipments that are used to exchange routing information and service policy (e.g., peer-to-peer (P2P) service acceleration policy) between the iSCP-based network and legacy networks.

(2) VNEs are required to process the time to live (TTL) value of incoming packets, as done by legacy packet network routers.

7.9 Routing

(1) For routing within a VNE, CEs are required to calculate the RIB within a VNE, taking into account the routing policy.

(2) For routing among VNEs, CEs are required to exchange the routing information among VNEs and calculate the RIB reflecting the route among VNEs.

(3) For routing between a VNE and an external network, CEs are required to exchange the routing information with any external network routing node connected with the VNE and to calculate the RIB reflecting the route between the VNE and the external network.

7.10 Forwarding

FEs are required to receive FIBs from the connected CEs and to forward the packets according to the FIBs.

8 Security considerations

Security considerations specific to iSCP are given in clause 7.7.

Bibliography

The following documents contain information that may be valuable to the reader of this Recommendation. They provide additional information about topics covered within this Recommendation, but are not essential for an understanding of this Recommendation.

[b-ITU-T Y-Sup.11] ITU-T Y.2600-series Recommendations – Supplement 11 (2010), *Supplement on scenarios for independent scalable control plane (iSCP) in future packet-based networks (FPBN)*.

[b-IETF RFC 3654] IETF RFC 3654 (2003), *Requirements for Separation of IP Control and Forwarding*.

[b-IETF RFC 3746] IETF RFC 3746 (2004), *Forwarding and Control Element Separation (ForCES) Framework*.

[b-IETF RFC 5810] IETF RFC 5810 (2010), *Forwarding and Control Element Separation (ForCES) Protocol Specification*.

[b-IETF RFC 5811] IETF RFC 5811 (2010), *SCTP-Based Transport Mapping Layer (TML) for the Forwarding and Control Element Separation (ForCES) Protocol*.

[b-IETF RFC 5812] IETF RFC 5812 (2010), *Forwarding and Control Element Separation (ForCES) Forwarding Element Model*.

[b-IETF RFC 5813] IETF RFC 5813 (2010), *Forwarding and Control Element Separation (ForCES) MIB*.

[b-IETF RFC 6041] IETF RFC 6041 (2010), *Forwarding and Control Element Separation (ForCES) Applicability Statement*.

[b-IETF RFC 6053] IETF RFC 6053 (2010), *Implementation Report for Forwarding and Control Element Separation (ForCES)*.

[b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.

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	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**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012