International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 11

(01/2010)

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

ITU-T Y.2600 series – Supplement on scenarios for independent scalable control plane (iSCP) in future packet-based networks (FPBN)

ITU-T Y-series Recommendations – Supplement 11

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
Future networks	**Y.2600–Y.2699**
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

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

Supplement 11 to ITU-T Y-series Recommendations

ITU-T Y.2600 series – Supplement on scenarios for independent scalable control plane (iSCP) in future packet-based networks (FPBN)

Summary

Supplement 11 to ITU-T Y-series Recommendations describes application scenarios provided by an independent scalable control plane (iSCP) which separates the control plane from the data plane in the future packet-based networks. This supplement can be used for providing guidance for defining iSCP requirements.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 11	2010-01-29	13

Keywords

Control plane, data plane, FPBN, scenarios, separation.

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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 11 to ITU-T Y-series Recommendations

ITU-T Y.2600 series – Supplement on scenarios for independent scalable control plane (iSCP) in future packet-based networks (FPBN)

1 Scope

This supplement describes the issues with current Internet Protocol (IP) networks and provides application scenarios and improvements provided by an independent scalable control plane (iSCP) which separates the control plane from the data plane in the future packet-based networks as described in [ITU-T Y.2601].

2 References

[ITU-T Y.2601] Recommendation ITU-T Y.2601 (2006), *Fundamental characteristics and requirements of future packet based networks*.

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

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

3 Terms and definitions

This supplement defines the following terms:

3.1 control element (CE): A control element is an entity which makes routing computation and decisions on Internet Protocol/multi-protocol label switching (IP/MPLS) forwarding table for one or multiple forwarding elements (FEs) based on a network-wide view according to network-level optimization and consistency objectives.

3.2 forwarding element (FE): A forwarding element (FE) is an entity which forwards the user data traffic according to the routing decisions of the CE(s).

3.3 management element (ME): A management element is an entity which manages control elements (CEs), service control elements (SCEs), forwarding elements (FEs) and service processing elements (SPEs), and partitions them into multiple re-constructible virtual network elements (VNEs).

3.4 service control element (SCE): A service control element is an entity which makes network service decisions on security, network address translation (NAT) and other layer 4 to 7 services for one or multiple service processing elements (SPEs) at the network level.

3.5 service processing element (SPE): A service processing element (SPE) is an entity which handles the user data traffic according to the network service decisions of the service control element(s) (SCEs), including deep packet inspection (DPI), network address translation (NAT), firewall, encryption/decryption, protocol conversion, monitoring, content processing and application acceleration, etc.

3.6 virtual network element (VNE): A virtual network element is a virtual heterogeneous cluster router consisting of multiple control elements (CEs), service control elements (SCEs), forwarding elements (FEs) and service processing elements (SPEs), which supports the appearance of a single functional network entity with high throughput for a given application service traffic (video, voice or data).

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

CE	Control Element
DPI	Deep Packet Inspection
FE	Forwarding Element
FIB	Forwarding Information Base
IP	Internet Protocol
iSCP	independent Scalable Control Plane
ME	Management Element
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
QoS	Quality of Service
RIB	Routing Information Base
SCE	Service Control Element
SPE	Service Processing Element
VNE	Virtual Network Element

5 Conventions

In this Supplement, the following convention is used:

The keyword "**Entity**" indicates CE, SCE, FE, SPE and ME.

6 Issues with current IP networks

The original IP networks were simply designed to support easy internetworking and best-effort communication for research use. Currently, IP networks have been widely deployed for commercial usage on a huge network scale and user scale, which will continue to increase rapidly. More and more new services, features and capabilities have been introduced into the IP networks.

Currently serving as the most important public data networks, the existing IP networks are encountering serious architectural problems as they evolve. These problems include issues related to capacity, scalability, controllability, security and QoS.

With the continued rapid increase in the number of users and their bandwidth and service requirements, the scalability and functionality for the network nodes and the whole network are of major concern. The control plane is becoming more and more complex. Scalability and controllability of the control plane, the management plane and the data plane of network nodes and the whole IP network are major challenges for future evolution.

The major reason 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 an IP network, the control plane and the data plane are integrated into a network node, and more and more control signalling and service functionalities are added into the network node. IP networks have become complex, thus making it difficult to maintain or extend.

Separation of the control plane from the data plane can alleviate scalability and controllability problems related to the current IP networks. Therefore, separation of the control plane and the data plane can improve the robustness of IP networks.

7 Overview of the iSCP

Figure 7-1 shows the relationship among three planes and the re-constructible components of the iSCP. The control plane contains mechanisms dealing with the network services and deciding the pathways for user traffic. These mechanisms will be implemented in CEs and SCEs. The data plane contains mechanisms forwarding and processing user traffic. These mechanisms will be implemented in FEs and SPEs. The management plane contains mechanisms dealing with the operation, administration, and management aspects of the iSCP network. These mechanisms will be implemented in MEs.

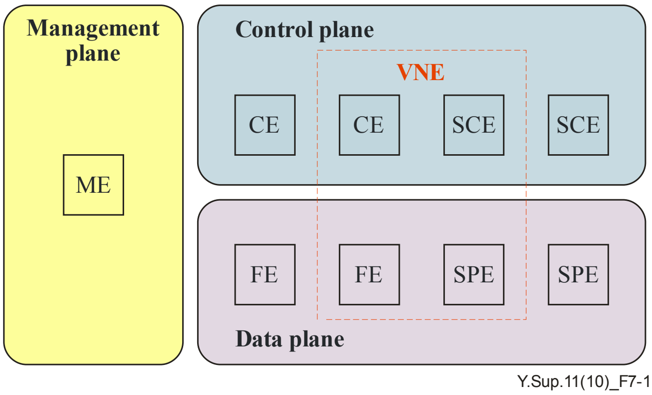

Figure 7-1 – Overview of the iSCP

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

In a VNE, one CE in the control plane can control one or a group of FE(s) in the data 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 communication with other CEs by routing protocols. Then CE(s) generate a forwarding information base (FIB) based on the RIB and download the FIB to the FE(s).

One SCE in the control plane can control associated SPE(s) in the data plane. The SCE will generate the rules for SPE(s) to process certain traffic. These rules are based on service policies, configured by ME(s) and maintained as a service control table. For example, service policies include quality of service (QoS) behaviour policies and access control policies. The SCE enforces the rules by setting service control table(s) to the associated SPE(s).

An FE in the data plane forwards incoming packets according to the FIB, which is generated and given 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 in the data plane handles incoming packets according to the service control table. The SPE receives and updates the service control table from the associated SCE(s), looks up the service control table, and handles packets according to the service control table. The SPE can process the packets such as NAT, encryption/decryption, protocol conversion and content processing, etc.

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

8 Application scenarios

8.1 Cluster router scenarios

A cluster router system consists of multiple entities, such as CE(s), SCE(s), FE(s), SPE(s) and ME(s). The ME(s) manage resources of all entities. And the ME(s) may partition them into multiple re-constructible VNEs.

A VNE is a virtual router which consists of multiple CE(s), SCE(s), FE(s) and SPE(s) which belong to the cluster router system. The VNE is a logical routing node (routing is only one hop) in a network, but not a subnet.

The VNE can support network scalability easily and provide high throughput with an appropriate number of entities for the application service traffic (video, voice or data).

8.1.1 Multiple entities connected with a switch fabric

As shown in Figure 8-1, multiple entities are connected with a switch fabric. The whole system can be partitioned into one or multiple VNEs. Every VNE uses the switch fabric to internally connect, and presents only one routing hop.

An SCE can support to add control entities related to the third-party value-added services. An SPE can support to add processing entities related to the third-party value-added services.

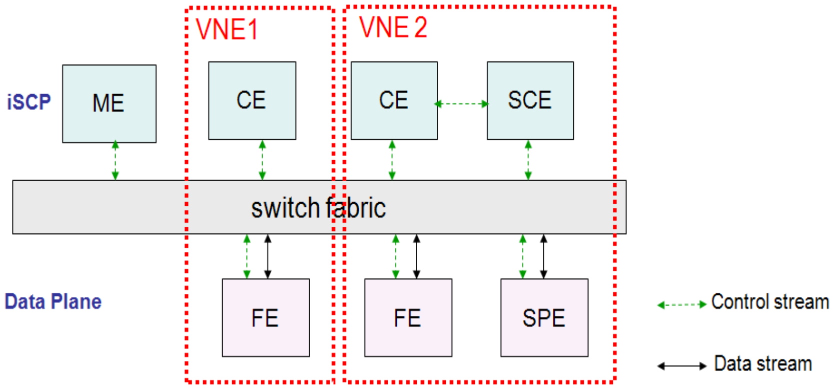

Figure 8-1 – Cluster router system consisting of multiple entities connected with a switch fabric

8.1.2 Multiple entities connected with an optical or Ethernet switch network

As shown in Figure 8-2, multiple entities are connected with an optical or Ethernet switch network. The whole system can be partitioned into one or multiple VNEs. Every VNE uses the optical or Ethernet switch network to internally connect, and presents only one routing hop.

An SCE can support to add control entities related to the third-party value-added services. An SPE can support to add processing entities related to the third-party value-added services.

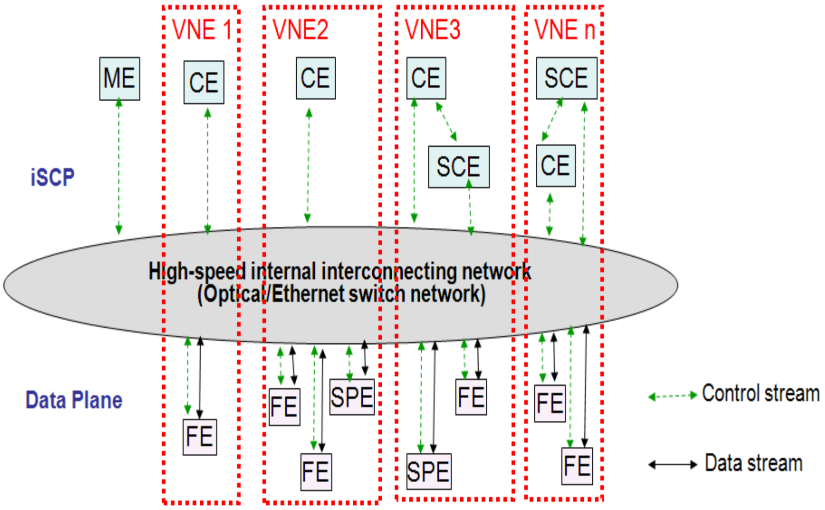

Figure 8-2 – Cluster router system consisting of multiple entities connected with an optical or Ethernet switch network

8.1.3 Multiple entities connected with an IP/MPLS network

As shown in Figure 8-3, multiple entities are connected with an IP/MPLS network. The whole system can be partitioned into one or multiple VNEs. Every VNE uses the IP/MPLS switch network to internally connect, and presents only one routing hop.

An SCE can support to add control entities related to the third-party value-added services. An SPE can support to add processing entities related to the third-party value-added services.

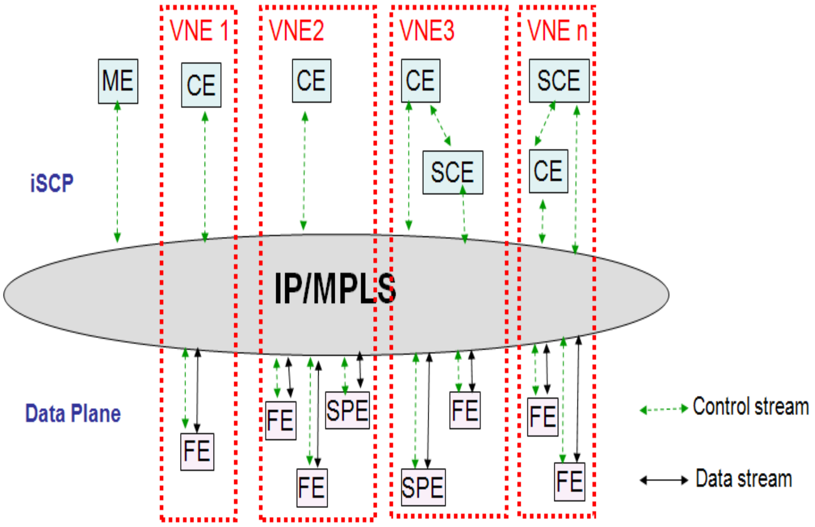

Figure 8-3 – Cluster router system consisting of multiple entities connected with an IP/MPLS network

8.2 CE/SCEs cooperation scenarios

An iSCP consists of independent control entities and is shared by all FEs in the iSCP network. The whole network represents an IP/MPLS network from an external view. Based on a distributed computing model, the iSCP can reduce the routing computation of all routers. Based on the whole network information, the iSCP can develop an intelligent network service.

8.2.1 One group of CE/SCEs working together

As shown in Figure 8-4, an iSCP network consists of multiple CE(s) and SCE(s), which are shared by all FEs and SPEs in a data plane network. The relationship among CEs and SCEs may be functionally-distributed, load-sharing or redundancy. CEs and SCEs can support flat or hierarchical architecture. In this case, some intra-domain interfaces for CE-CE, CE-SCE and SCE-SCE need to be defined for intra-domain communication.

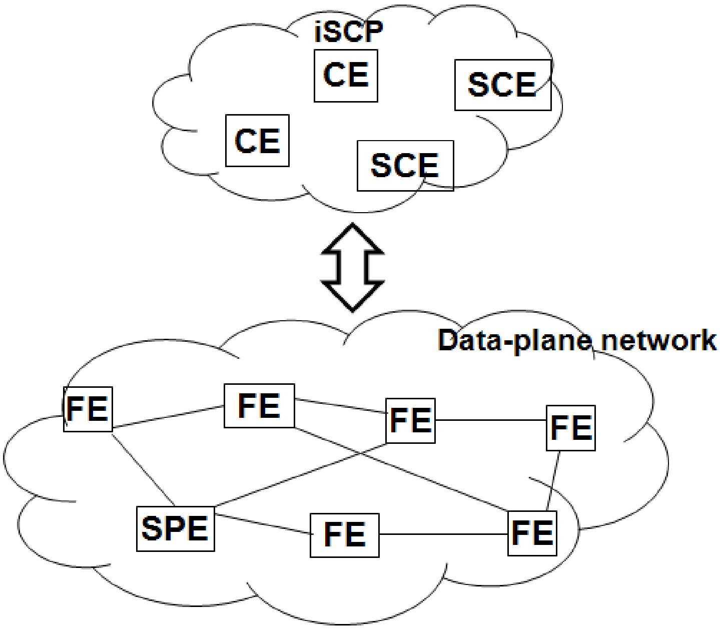

Figure 8-4 – A shared iSCP for a data plane network

8.2.2 Several groups of CE/SCEs working together

As shown in Figure 8-5, there can be multiple iSCP networks and data plane networks, and each iSCP network is shared by a network area. In this case, some inter-domain interfaces for CE-CE, SCE-CE and SCE-SCE need to be defined for inter-domain communication.

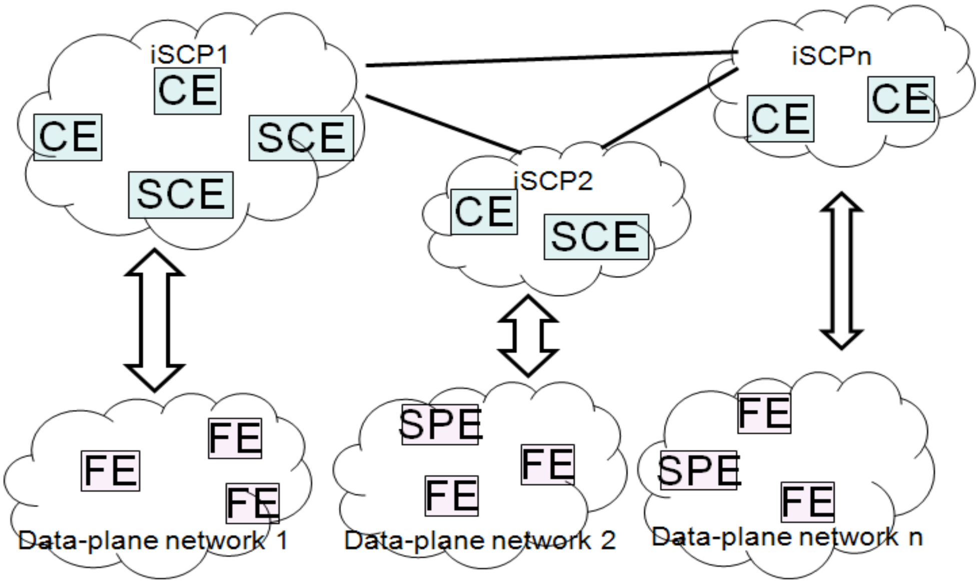

Figure 8-5 – Signalling network consisting of multiple shared iSCPs for multiple data plane networks

8.3 Configuration scenarios

8.3.1 Topology information configuration

8.3.1.1 Setting the topology information from a data plane

As shown in Figure 8-6, a data plane network consists of multiple FEs and SPEs which are controlled by one or multiple CE(s) and SCE(s). FEs and SPEs in the data plane bind to adjacent FEs and monitor the status of the network by using any adjacent detection function, and notify one or multiple CEs and SCEs.

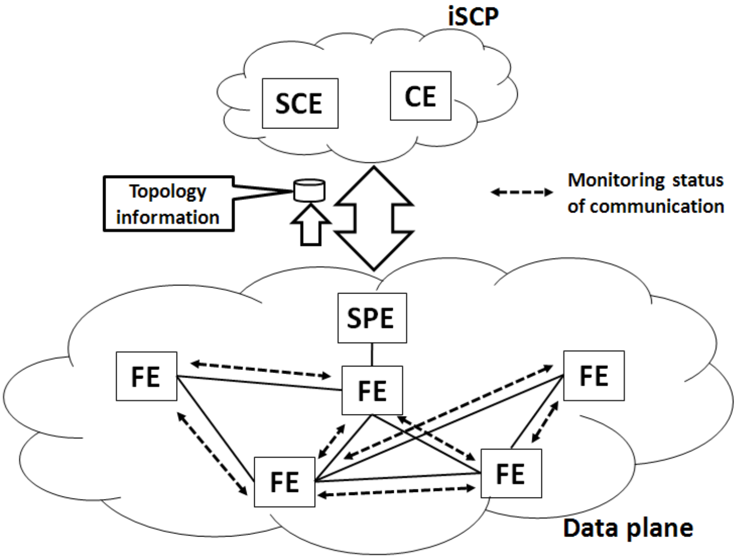

Figure 8-6 – Setting the topology information from a data plane

8.3.1.2 Setting the topology information from a management plane

As shown in Figure 8-7, an ME sends the topology information to CEs every time the operator updates the topology information.

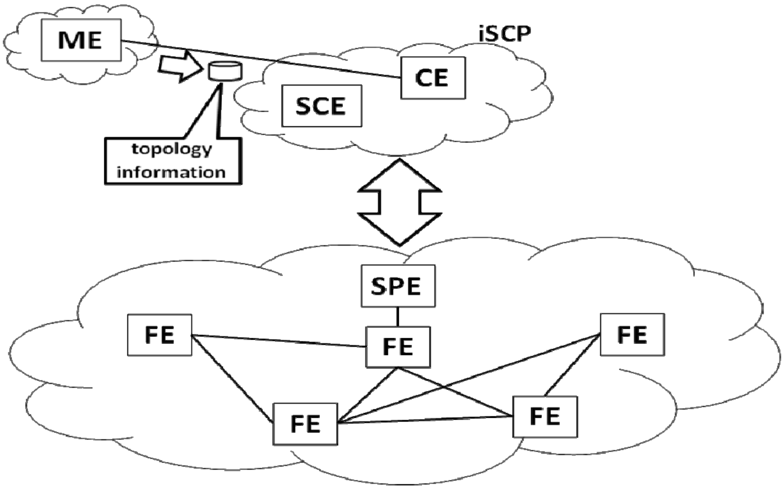

Figure 8-7 – Setting the topology information from a management plane

8.3.2 Service configuration

8.3.2.1 Setting the service configuration from CEs and/or SCEs

As shown in Figure 8-8, FEs and/or SPEs can be configured by CEs and/or SCEs. CEs and/or SCEs can automatically configure and deploy services to all FEs and/or SPEs. CEs and/or SCEs manage an FE and/or SPE's service configuration, automatically decompose the VNE service configuration into a configuration of each FE and/or SPE, and compute a service control table for each FE and/or SPE. Each FE or SPE in time reports local link/interface status and change to the CE or SCE, and receives from the CE or SCE a service control table to achieve the automatic deployment of a service.

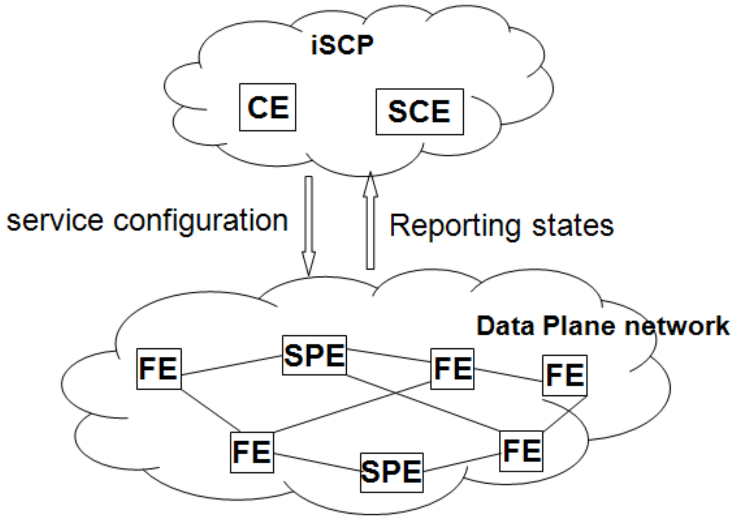

Figure 8-8 – Setting the service configuration from CEs and/or SCEs

8.3.2.2 Setting the service configuration from an ME

As shown in Figure 8-9, FEs and/or SPEs can be indirectly configured by an ME. The ME sends service configuration information, which is set by the network operator or obtained from configuration files, to CEs and/or SCEs. Then the CEs and/or SCEs decompose and send the configuration information to FEs and/or SPEs to set their interfaces and service control table entries, etc.

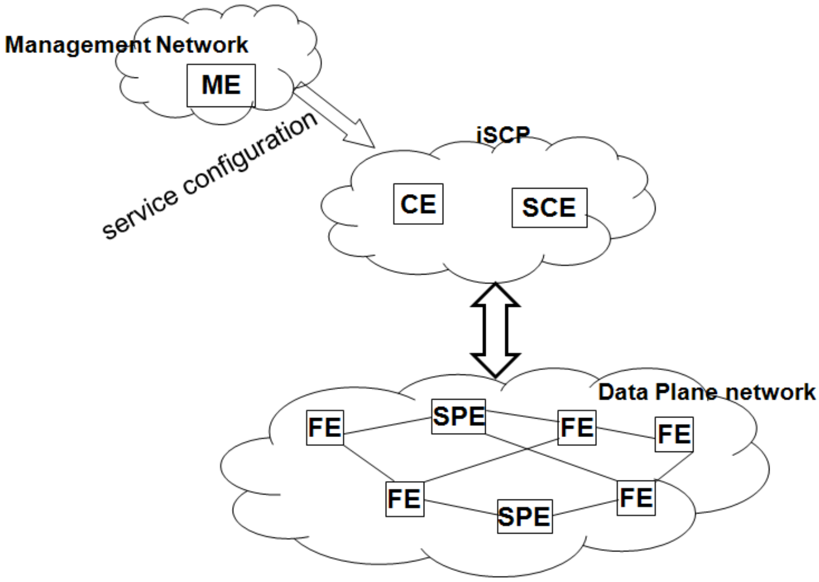

Figure 8-9 – Setting the service configuration from an ME

8.4 Forwarding and processing scenarios

8.4.1 Forwarding data packets

8.4.1.1 Forwarding data packets based on an FIB

As shown in Figure 8-10, FEs in the data plane forward the data packets based on FIBs. FIBs are generated in the following steps:

1) Communication channels between CE(s) and FE(s) are established.

2) The CE collects the link status and topology information from neighbouring CEs, FEs and MEs.

3) The CE computes the RIB.

4) The CE respectively computes the FIB for each connected FE according to the RIB.

5) The CE respectively sends the FIB to the corresponding FE.

Additionally, FEs can also forward specific data packets based on the combination of the data packet header fields, e.g., 5-tuple other than the destination address, so that multiple data packets with the same destination address can be forwarded through different routes.

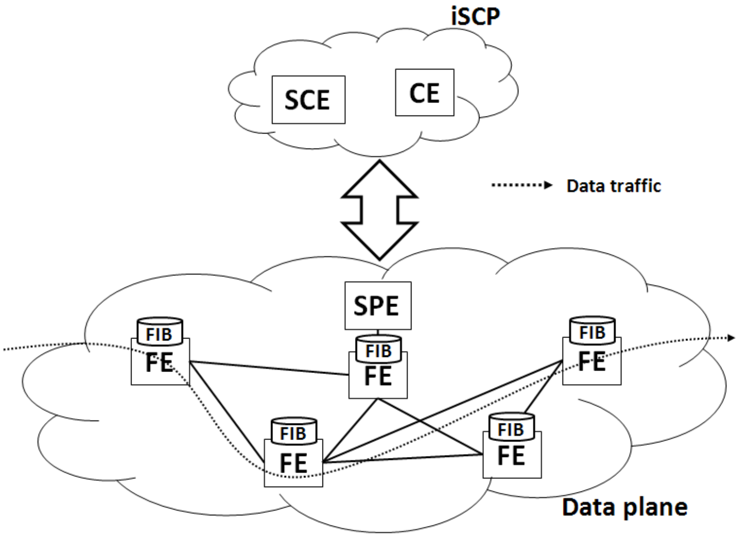

Figure 8-10 – Forwarding data packets based on an FIB

8.4.1.2 Forwarding data packets based on a specific routing policy

As shown in Figure 8-11, FEs in the data plane can forward a specific data packet to a specific next hop based on the destination address and/or other fields in the data packet header. Such specific routing policies are generated by CE(s) based on the topology information. CE easily controls the forwarding path by the routing policy because the topology information of the data plane network has been gathered.

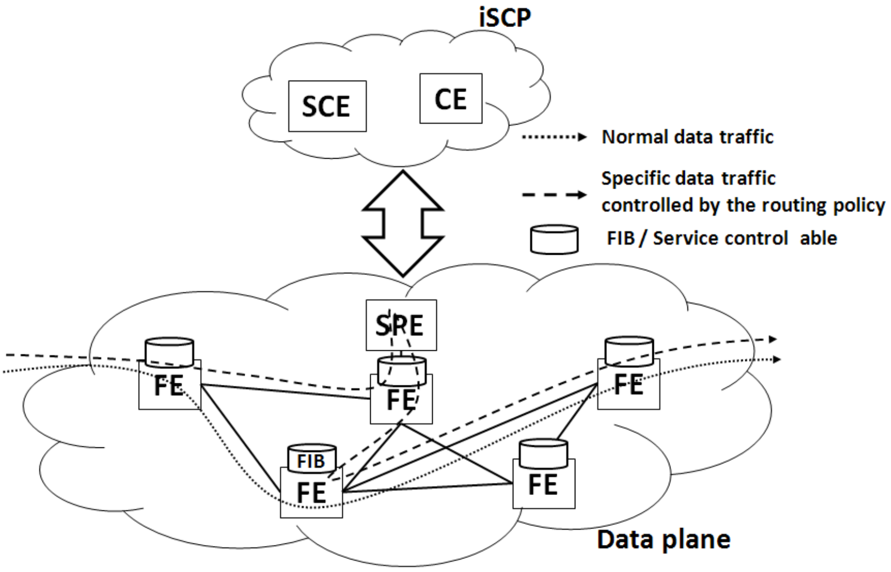

Figure 1

Figure 8-11 – Forwarding data packets based on a specific routing policy

8.4.2 Processing data packet

As shown in Figure 8-12, SPE(s) can process a specific data packet which is forwarded along the policy routing path according to the service demand from the SCE(s).

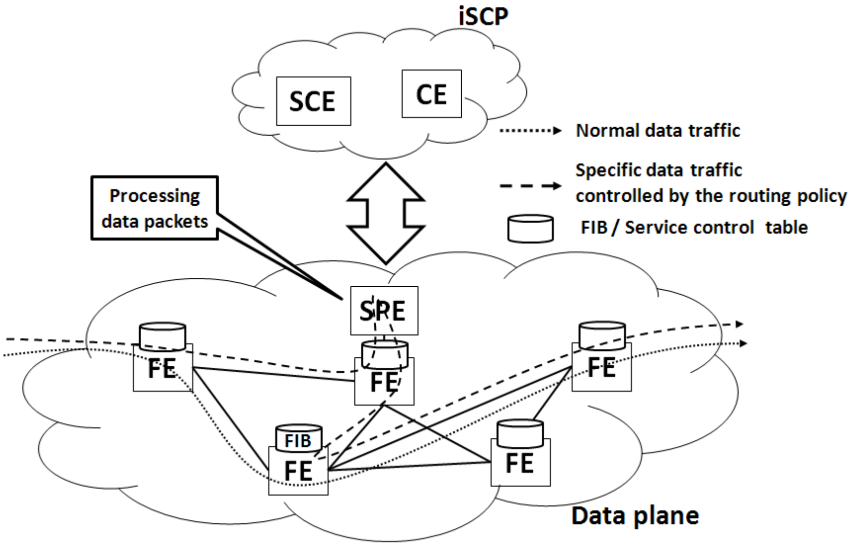

Figure 8-12 – Processing data packets based on a specific service policy

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, 2010