International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2622

(07/2012)

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

Next Generation Networks – Packet-based Networks

Architecture of an independent scalable control plane in future packet based networks

Recommendation ITU-T Y.2622

ITU-T

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
Packet-based Networks	**Y.2600–Y.2699**
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2622

Architecture of an independent scalable control plane in future packet based networks

Summary

Recommendation ITU-T Y.2622 describes the functional architecture of an independent scalable control plane (iSCP) that is achieved by separating the control plane from the data plane in future packet based networks (FPBNs). Basic functional components and reference points of an iSCP are illustrated.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2622	2012-07-29	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

Recommendation ITU-T Y.2622

Architecture of an independent scalable control plane in future packet based networks

1 Scope

This Recommendation describes the architecture, basic functional components, and reference points of an independent scalable control plane (iSCP) that is achieved by separating the control plane from the data plane in future packet based networks (FPBN), as described in [ITU-T Y.2621].

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.2621] Recommendation ITU-T Y.2621 (2011), *Requirements for an independent, scalable control plane in 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 future packet based network (FPBN) [ITU-T Y.2621]: A network architecture providing the topmost layer(s) of the transport stratum as defined in [ITU-T Y.2011].

3.1.4 independent scalable control plane (iSCP) [ITU-T Y.2621]: An architectural approach of future packet based networks (FPBNs) which consists of separating the control plane from the data plane.

3.1.5 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

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BGP Border Gateway Protocol

CE	Control Element
FE	Forwarding Element
FIB	Forwarding Information Base
FPBN	Future Packet Based Networks
iSCP	independent Scalable Control Plane
ME	Management Element
MIB	Management Information Base
OSPF	Open Shortest Path First
QoS	Quality of Service
RIB	Routing Information Base
SCE	Service Control Element
SPE	Service Processing Element
VNE	Virtual Network Element

5 Conventions

In this Recommendation, the following conventions are used:

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

6 iSCP architecture

The high level requirements stated in [ITU-T Y.2621] necessitate defining the following reconstructible components for the iSCP architecture: the control plane, data plane, management plane, control elements (CEs), service control elements (SCEs), forwarding elements (FEs), service processing elements (SPEs), and management elements (MEs).

Figure 6-1 shows the relationship between the control plane, data plane, and management plane, and the relationship of the reconstructible components. Multiple MEs, CEs, SCEs, FEs, and SPEs can form a virtual network element (VNE).

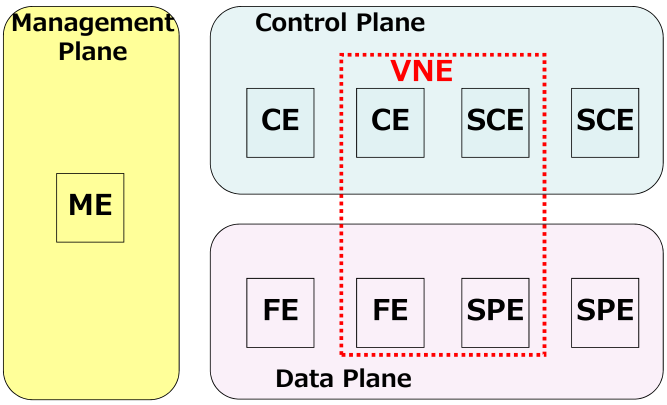

Figure 6-1 – Three planes and reconstructible components

The control plane of an iSCP contains mechanisms for operating the packets and deciding the pathways for user traffic. These mechanisms are implemented in the CEs and SCEs. The data plane of an iSCP contains mechanisms for forwarding and processing user traffic and/or control traffic. These mechanisms are implemented in the FEs and SPEs. The management plane of an iSCP contains mechanisms for 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 are implemented in the MEs.

Figure 6-2 illustrates the iSCP functional architecture representing the entities of iSCP and the reference points among the entities.

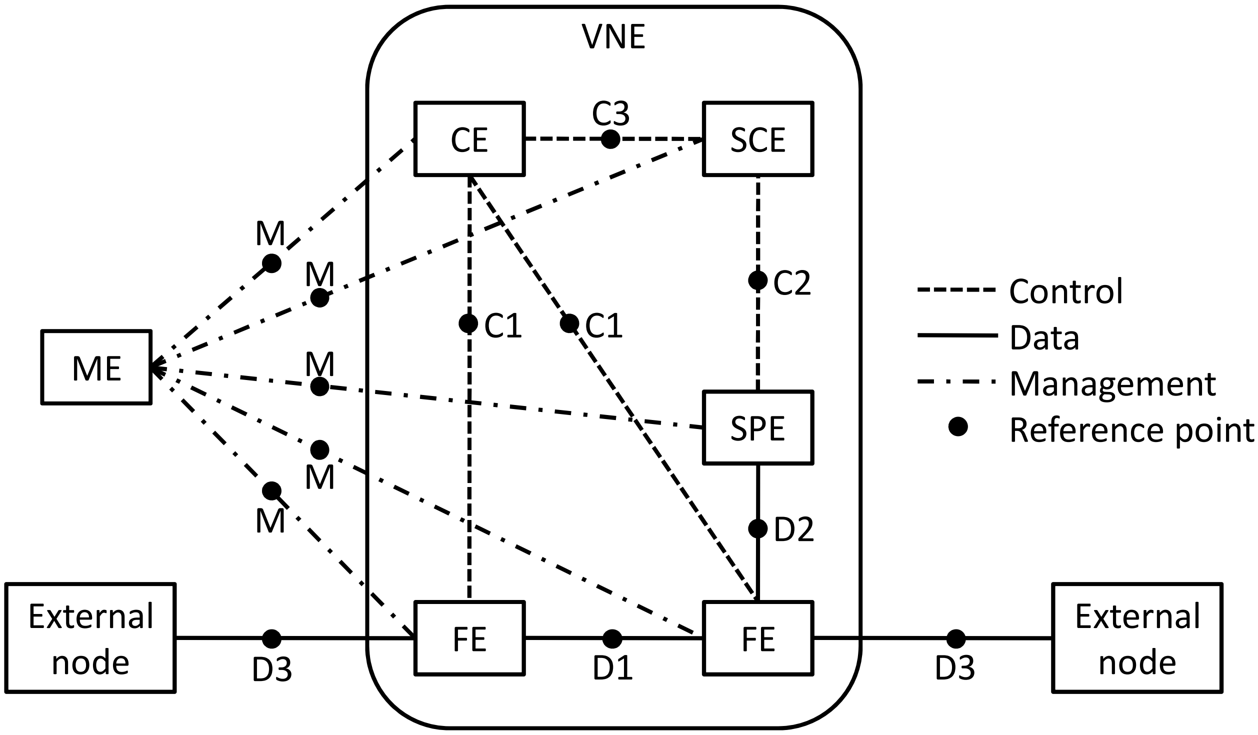

Figure 6-2 – iSCP functional architecture

The iSCP functional architecture provides two basic operations, VNE configuration and VNE operation. The VNE configuration includes: composing a VNE from CEs, SCEs, FEs, and SPEs based on configuration information from MEs; changing the structure of the VNE depending on the required capacity and flexibility; and breaking up the VNE. The VNE operation involves operating the constructed VNE as a single conventional network entity, e.g., a router.

The iSCP architecture provides three types of reference points, control type reference point C, data type reference point D, and management type reference point M. The control type reference point C is used to exchange control information and includes reference points C1, C2, and C3. Reference point C1 is used between CEs and FEs, reference point C2 is used between SCEs and SPEs, and reference point C3 is used between CEs and SCEs. The data type reference point D is used to forward packets and includes reference points D1, D2, and D3. Reference point D1 is used between FEs and FEs, reference point D2 is used between FEs and SPEs, and reference point D3 is used between FEs and external nodes. The management type reference point M is used to exchange configuration and management information between MEs and CEs/FEs/SCEs/SPEs.

6.1 Virtual network element (VNE)

The VNE is a virtual entity composed of multiple CEs, SCEs, FEs, and SPEs based on the configuration information from MEs. The number of individual entities used for the VNE can vary depending on the required capacity and flexibility. The VNE operates as a single conventional network entity, e.g., a router. The VNE hides its internal organization from external nodes and represents a single point of management to entities outside the VNE. Besides management information bases (MIBs) of each entity in the VNE, there are also MIBs for the whole VNE. The MIBs of the VNE are held and managed by the MEs.

6.2 Control element (CE)

One VNE can include one or several CEs. The interfaces among the CEs, which are needed when several CEs cooperate with each other within the VNE, will not be defined in this Recommendation.

The CE provides the capability to join and leave one VNE based on configuration information from the ME(s).

The CE instructs one or a group of FE(s) on how to process packets. The CE generates the packet-forwarding rules for FE(s) and downloads the forwarding rules to the FE(s). To generate these forwarding rules, the CE maintains necessary information in a routing information base (RIB) to compute the most suitable route for incoming packets. The CE updates the RIB in several ways, e.g., by communicating with external nodes through routing protocols via FE(s), by receiving the topology information within the VNE from FE(s), or by receiving the static route configuration from ME(s). Also, the CE maintains routing policies for generating the forwarding rules for FE(s), which indicate specific routes for specific packets. The CE receives such routing policies from ME(s) upon request of network operators, or from SCE(s) upon request from the service control of the SCE(s).

The CE manages the CE state information such as entity status and operating status of the CE itself and maintains the MIBs of the CE. The CE allows ME(s) to access these MIBs.

Figure 6-3 shows the functions of the CE and its related reference points.

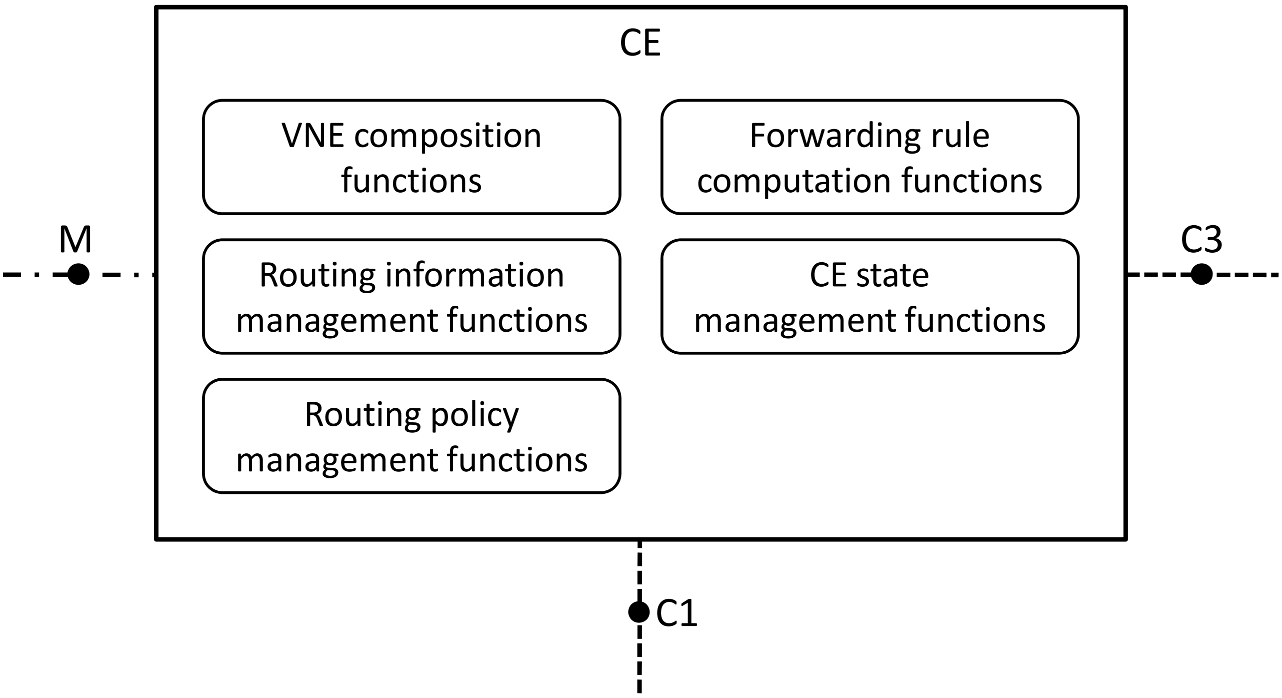

Figure 6-3 – Control element

6.2.1 VNE composition functions

The VNE composition functions support the CE in composing the VNE. The VNE composition functions interact with ME(s) to receive the configuration information through reference point M. The configuration information indicates which other entities the CE should be connected to. Based on the configuration information, the VNE composition functions establish or terminate the control sessions with FE(s) through reference point C1 or with SCE(s) through reference point C3.

6.2.2 Routing information management functions

The routing information management functions provide the capabilities to collect and store the routing information required for the VNE to forward packets. The routing information management functions collect the routing information in several ways, e.g., by communicating with external nodes through routing protocols via FE(s) using reference point C1, by receiving the topology information within the VNE from FE(s) through reference point C1, and by receiving the static route configuration from ME(s) through reference point M. The routing information management functions store the collected routing information in the RIB.

6.2.3 Routing policy management functions

The routing policy management functions provide the capabilities to receive and store the routing policies required for the VNE to forward specific packets on a specific route. The routing policy management functions receive the routing policies from ME(s) through reference point M upon request of network operators or from SCE(s) through reference point C3 upon request from the service control of the SCE(s). The routing policy management functions store the received routing policies in the routing policy database.

6.2.4 Forwarding rule computation functions

The forwarding rule computation functions generate the forwarding rules for FE(s) to forward packets based on the information of the RIB and the routing policy database. The forwarding rule computation functions download the generated forwarding rules to the FE(s) through reference point C1.

6.2.5 CE state management functions

The CE state management functions are responsible for managing CE state information such as the entity status and operating status of the CE itself. The CE state management functions store the CE state information in the MIBs of the CE. The CE state management functions respond to the accesses from ME(s) to the MIBs of the CE through reference point M.

6.3 Service control element (SCE)

One VNE can include one or several SCEs. The interfaces among the SCEs, which are needed when several SCEs cooperate with each other within the VNE, will not be defined in this Recommendation.

The SCE provides the capabilities to join and leave one VNE based on configuration information from ME(s).

The SCE instructs associated SPE(s) on how to process packets. The SCE generates the processing rules for SPE(s) to process packets, and downloads the processing rules to the SPE(s). The SCE maintains service policies to generate the processing rules for SPE(s). The SCE receives such service policies from ME(s) upon request of network operators. For example, service policies include quality of service (QoS) behaviour policies and access control policies. If the service policies need to indicate a specific route for specific packets, the SCE generates the appropriate routing policies and sends the generated routing policies to the CE(s).

The SCE manages the SCE state information such as entity status and operating status of the SCE itself and maintains the MIBs of the SCE. The SCE allows ME(s) to access these MIBs.

Figure 6-4 shows the functions of the SCE and its related reference points.

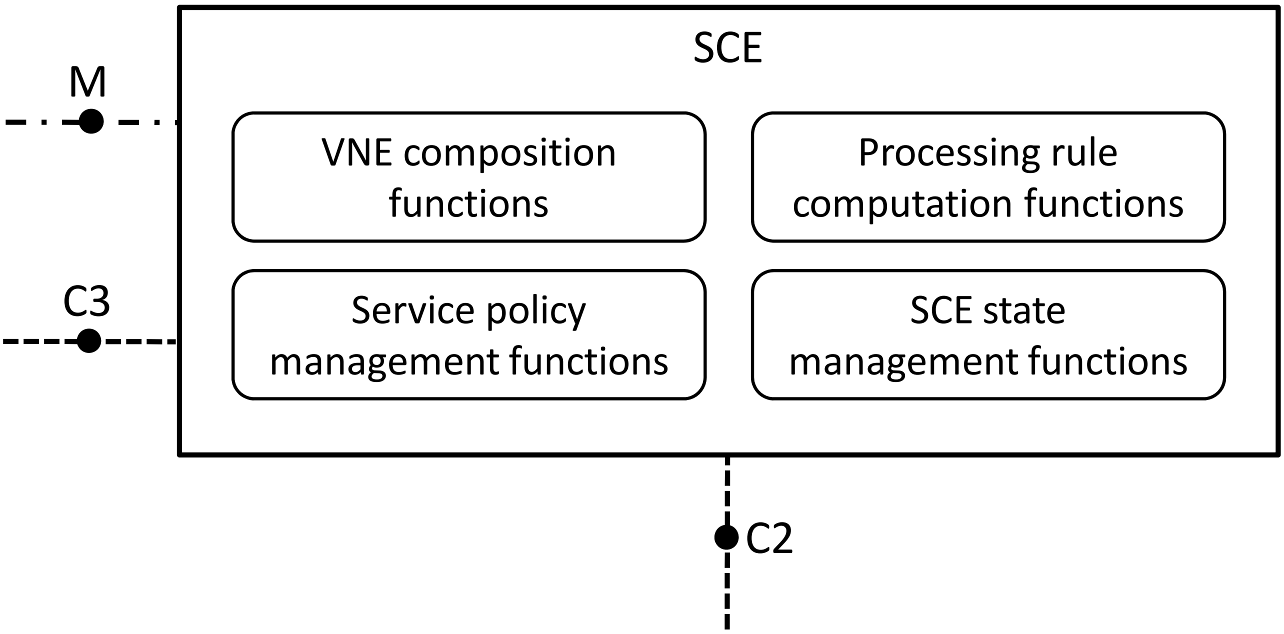

Figure 6-4 – Service control element

6.3.1 VNE composition functions

The VNE composition functions support the SCE in composing the VNE. The VNE composition functions interact with ME(s) to receive the configuration information through reference point M. The configuration information indicates which other entities the SCE should be connected to. Based on the configuration information, the VNE composition functions establish or terminate the control sessions with SPE(s) through reference point C2 or with CE(s) through reference point C3.

6.3.2 Service policy management functions

The service policy management functions provide the capabilities to receive and store the service policies required for SPE(s) to process specific packets. The service policy management functions receive the service policies from ME(s) through reference point M upon request of network operators. The service policy management functions store the received service policies in the service policy database.

6.3.3 Processing rule computation functions

The processing rule computation functions generate the processing rules for SPE(s) to process packets based on the information in the service policy database. The processing rule computation functions download the generated processing rules to the SPE(s) through reference point C2. If the service policies need to indicate a specific route for specific packets, the processing rule computation functions generate the appropriate routing policies and send the generated routing policies to CE(s) through reference point C3.

6.3.4 SCE state management functions

The SCE state management functions are responsible for managing SCE state information such as entity status and operating status of the SCE itself. The SCE state management functions store the SCE state information in the MIBs of the SCE. The SCE state management functions respond to the accesses from ME(s) to the MIBs of the SCE through reference point M.

6.4 Forwarding element (FE)

The FE provides the capabilities to join and leave one VNE based on configuration information from ME(s).

The FE forwards incoming packets according to the forwarding rules generated and given by CE(s). The forwarding rules consist of the information needed for the FE to forward incoming packets, e.g., information on the packets' next hop. The FE maintains the forwarding rules in a forwarding information base (FIB) and updates the FIB by receiving the latest forwarding rules from CE(s).

The FE manages the FE state information such as entity status and operating status of the FE itself and maintains the MIBs of the FE. The FE allows ME(s) to access these MIBs.

Figure 6-5 shows the functions of the FE and its related reference points.

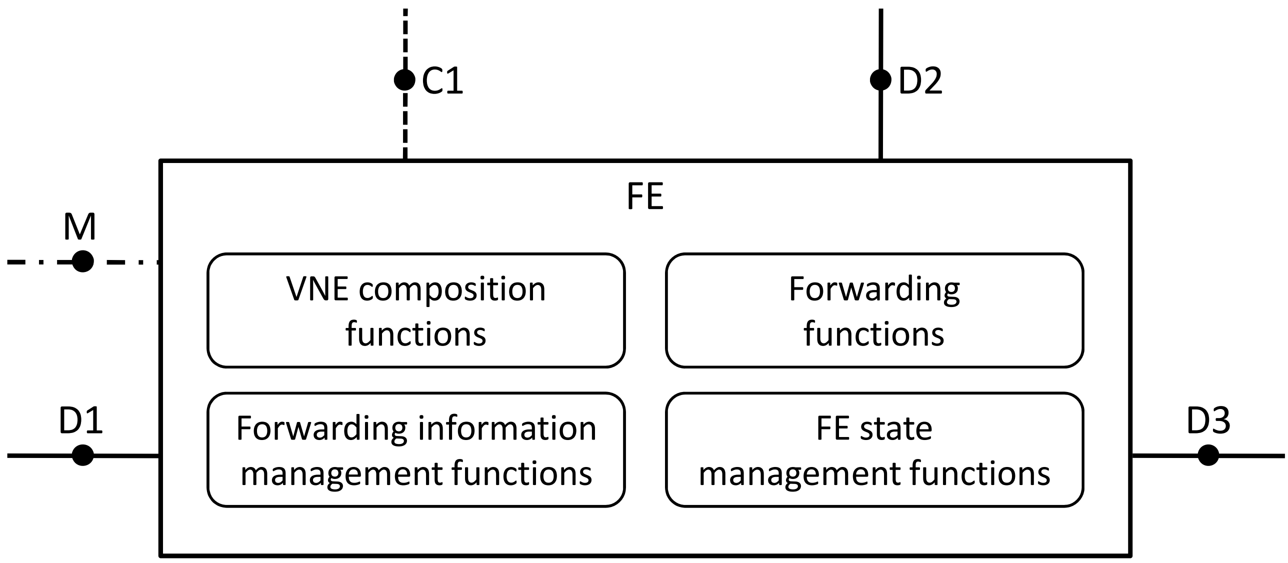

Figure 6-5 – Forwarding element

6.4.1 VNE composition functions

The VNE composition functions support the FE in composing the VNE. The VNE composition functions interact with ME(s) to receive the configuration information through reference point M. The configuration information indicates which other entities the FE should be connected to. Based on the configuration information, the VNE composition functions establish or terminate the control sessions with CE(s) through reference point C1.

6.4.2 Forwarding information management functions

The forwarding information management functions provide the capabilities to collect and store the forwarding rules for the FE to forward incoming packets. The forwarding information management functions receive the latest forwarding rules from CE(s) through reference point C1. The forwarding information management functions store the collected forwarding rules in the FIB.

6.4.3 Forwarding functions

The forwarding functions provide the capabilities to forward incoming packets according to the information in the FIB. The forwarding functions receive packets from or send packets to the connected FE(s) through reference point D1, the connected SPE(s) through reference point D2, the connected external node(s) through reference point D3, and the connected CE(s) through reference point C1. Normal data packets are transmitted only through reference points D1 and D3. Specific data packets that are required to be processed by the connected SPE(s) are transmitted not only through reference points D1 and D3 but also D2. Specific control packets, e.g., open shortest path first (OSPF) protocol packets and border gateway protocol (BGP) packets are transmitted through reference points D3 and C1 because such packets are redirected from the data plane to the control plane at the FE(s) situated on the edges of the VNE.

6.4.4 FE state management functions

The FE state management functions are responsible for managing FE state information such as entity status and operating status of the FE itself. The FE state management functions store the FE state information in the MIBs of the FE. The FE state management functions respond to the accesses from ME(s) to the MIBs of the FE through reference point M.

6.5 Service processing element (SPE)

The SPE provides the capabilities to join and leave one VNE based on configuration information from ME(s).

The SPE processes incoming packets from the connected FE(s) according to the processing rules generated and given by SCE(s). The processing rules consist of the information needed for the SPE to process incoming packets, e.g., QoS behaviour information and access control information. The SPE maintains the processing rules in a service control table, and updates the service control table by receiving the latest processing rules from SCE(s).

The SPE manages the SPE state information such as entity status and operating status of the SPE itself and maintains the MIBs of the SPE. The SPE allows ME(s) to access these MIBs.

Figure 6-6 shows the functions of the SPE and its related reference points.

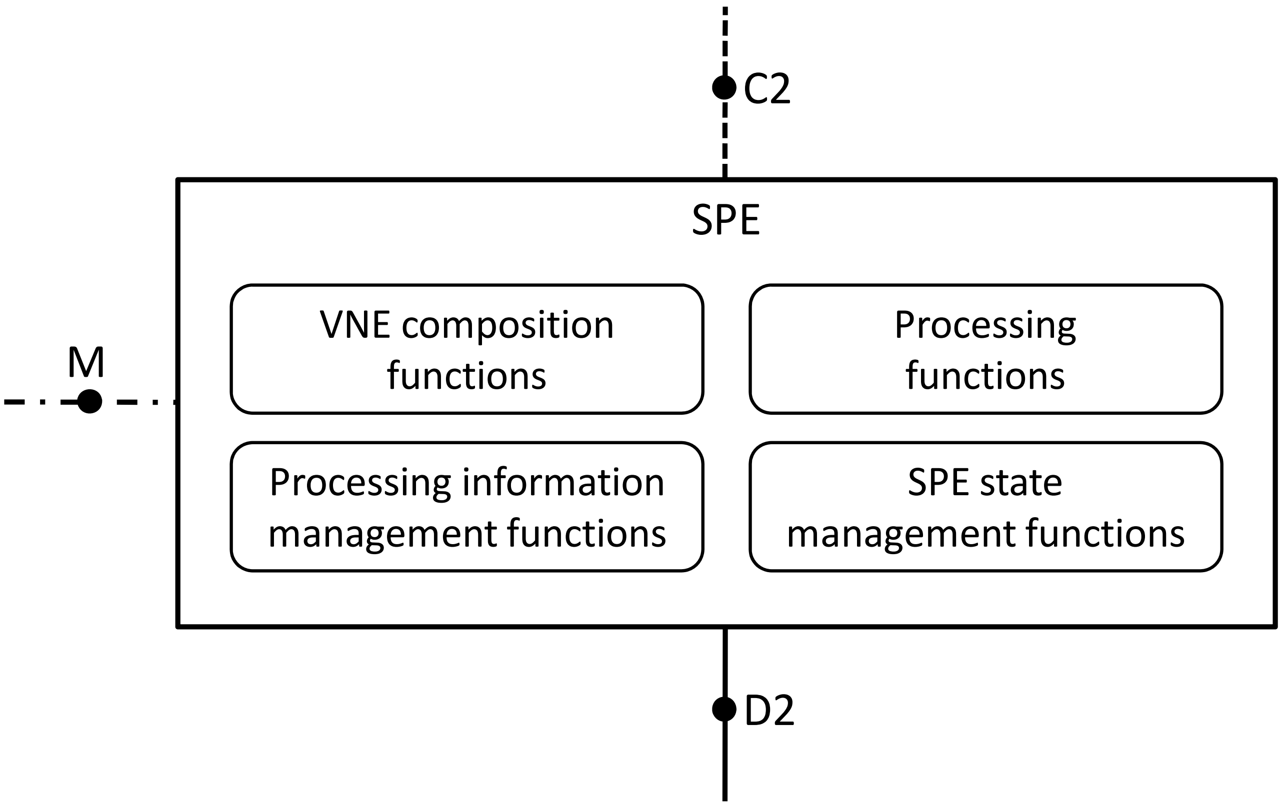

Figure 6-6 – Service processing element

6.5.1 VNE composition functions

The VNE composition functions support the SPE in composing the VNE. The VNE composition functions interact with ME(s) to receive the configuration information through reference point M. The configuration information indicates which other entities the SPE should be connected to. Based on the configuration information, the VNE composition functions establish or terminate the control sessions with SCE(s) through reference point C2.

6.5.2 Processing information management functions

The processing information management functions provide the capabilities to collect and store the processing rules for the SPE to process incoming packets. The processing information management functions receive the latest processing rules from SCE(s) through reference point C2. The processing information management functions store the collected processing rules in the service control table.

6.5.3 Processing functions

The processing functions provide the capabilities to process incoming packets according to the information in the service control table. The processing functions receive packets from or send the processed packets to the connected FE(s) through reference point D2. Specific data packets that are required to be processed by the SPE are sent from the connected FE(s) through reference point D2. If the processed data packets have to reach other destinations, the processed packets are returned to the connected FE(s) through reference point D2.

6.5.4 SPE state management functions

The SPE state management functions are responsible for managing the SPE state information such as entity status and operating status of the SPE itself. The SPE state management functions store the SPE state information in the MIBs of the SPE. The SPE state management functions respond to the accesses from ME(s) to the MIBs of the SPE through reference point M.

6.6 Management element (ME)

The ME provides the capabilities to manage CE(s), SCE(s), FE(s), and SPE(s) and partition them into multiple reconstructible VNEs.

The ME maintains VNE composition information set by network operators that describes the relationships between VNEs and the entities composing the VNEs. According to the VNE composition information, the ME sends VNE configurations to CE(s), SCE(s), FE(s), and SPE(s).

Upon request of network operators, the ME sends several kinds of operation configurations, e.g., static route configuration, routing policies, and service policies, to CE(s) or SCE(s).

The ME monitors the state information of VNE(s), CE(s), SCE(s), FE(s), and SPE(s) by accessing the MIBs of these entities.

The ME manages the state information of all VNEs such as entity status and operating status of the VNEs, and maintains the MIBs of the VNEs.

Figure 6-7 shows the functions of the ME and its related reference points.

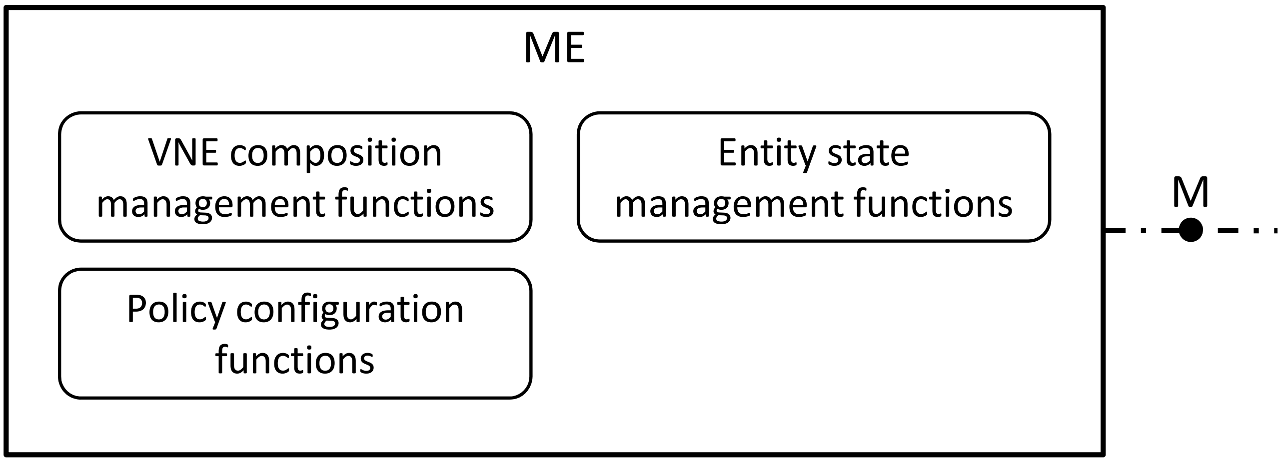

Figure 6-7 – Management element

6.6.1 VNE composition management functions

The VNE composition management functions store the VNE composition information set by network operators, which describes the relationships between VNEs and the entities composing the VNEs, in the VNE composition information database. According to the VNE composition information, the VNE composition management functions send VNE configurations to CE(s), SCE(s), FE(s), and SPE(s) through reference point M.

6.6.2 Policy configuration functions

The policy configuration functions provide the capabilities to send several kinds of policy configurations upon request of network operators. For example, the policy configuration functions send static route configurations or routing policies to CE(s), or service policies to SCE(s), through reference point M.

6.6.3 Entity state management functions

The entity state management functions provide the capabilities to monitor the state information of VNE(s), CE(s), SCE(s), FE(s), and SPE(s) by accessing the MIBs of these entities.

The state management functions retrieve the information in the MIBs on the CE(s), SCE(s), FE(s), and SPE(s) through reference point M.

The entity state management functions are responsible for managing the VNE state information such as entity status and operating status of the VNE as a single network entity. The entity state management functions store the VNE state information in the MIBs of all VNEs.

7 Reference points

The reference points within the iSCP architecture are as follows:

C1 Reference point between CEs and FEs. Through this reference point, CEs establish or terminate control sessions with FEs, collect routing information from FEs, and download forwarding rules to FEs.

C2 Reference point between SCEs and SPEs. Through this reference point, SCEs establish or terminate control sessions with SPEs and download processing rules to SPEs.

C3 Reference point between CEs and SCEs. Through this reference point, CEs establish or terminate control sessions with SCEs and receive routing policies from SCEs.

D1 Reference point among FEs in same VNE. Through this reference point, FEs receive packets from or send packets to connected FEs.

D2 Reference point between FEs and SPEs. Through this reference point, FEs send specific data packets that need to be processed by SPEs to the SPEs and receive processed packets from the SPEs.

D3 Reference point between FEs and external nodes. Through this reference point, FEs receive packets from or send packets to external nodes.

M Reference point between MEs and CEs/SCEs/FEs/SPEs. Through this reference point, MEs send VNE configurations to CEs/SCEs/FEs/SPEs, send static route configurations or routing policies to CEs, send service policies to SCEs, and retrieve information in MIBs on CEs/SCEs/FEs/SPEs.

8 Security considerations

The security requirements within the iSCP architecture are addressed by the security requirements in [ITU-T Y.2621].

Appendix I

Procedures related to iSCP

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

This appendix describes a procedure for CE/SCE failover.

The iSCP architecture separates the control plane from the data plane in the FPBNs, and one control plane element, CE/SCE, consolidates and controls multiple data plane elements, FEs/SPEs. Under this architecture, if faults occur in the CE/SCE, and the CE/SCE become unable to serve a control function, all of the FEs/SPEs controlled by the CE/SCE will be affected. Therefore, it is important to ensure the high reliability of the CE/SCE in the iSCP architecture.

One of the standard ways to respond to a CE/SCE fault is to take a redundant configuration of CEs/SCEs. This means that network operators provide some standby CEs/SCEs for the active CEs/SCEs. If faults occur in any of the active CEs/SCEs, the operation of the failed CE/SCE will be continued in any of the standby CEs/SCEs. The entire iSCP based network usually has multiple VNEs, and each active CE/SCE belongs to a VNE, but none of the standby CEs/SCEs belong to a VNE. When faults occur in any of the active CEs/SCEs, a standby CE/SCE will then become an active CE/SCE in the VNE that includes the failed CE/SCE. This means the active CEs/SCEs in the existing VNEs share the standby CEs/SCEs. Because each VNE does not need to have exclusive redundant CEs/SCEs, network operators can adopt a cost-efficient redundant configuration.

In an iSCP based network, the ME maintains VNE composition information describing the relationships between VNEs and the entities composing the VNEs, and it monitors the state information of each element. Therefore, the ME should be responsible for detecting CE/SCE faults and conducting CE/SCE failover operations. Figure I.1 shows an example of the CE/SCE failover flows describing how the CE/SCE fault can be handled.

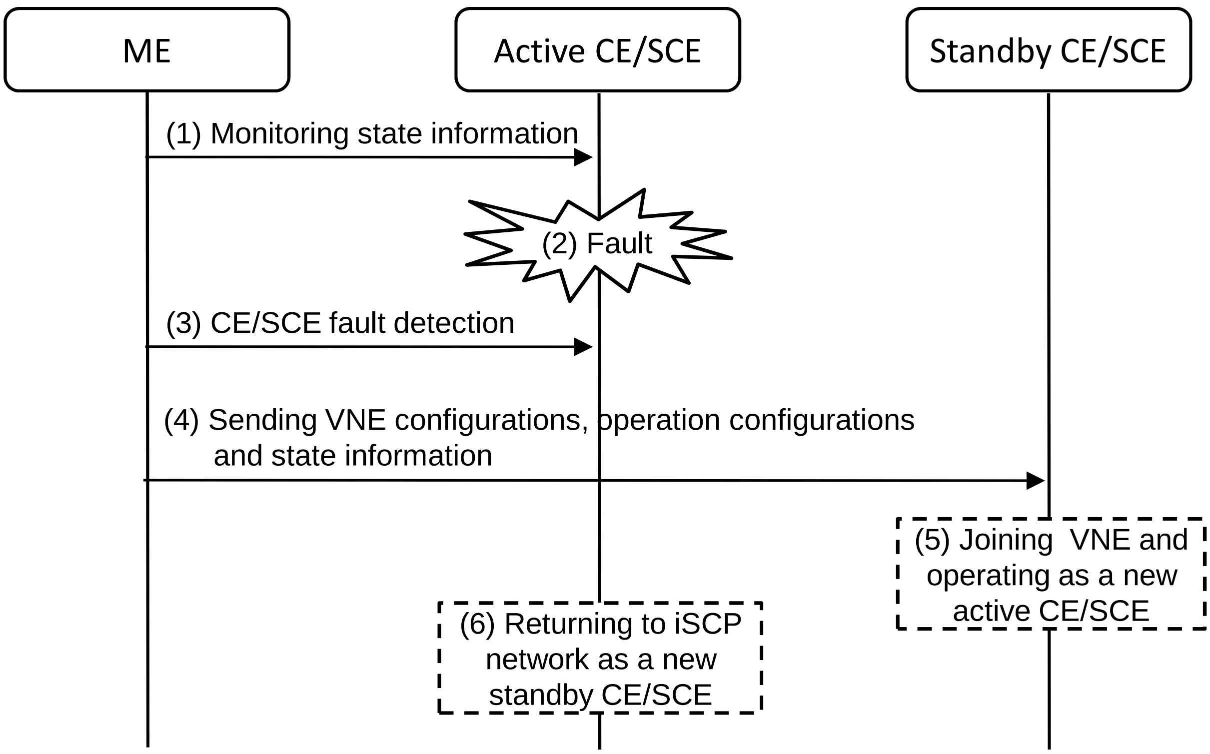

Figure I.1 – Example of CE/SCE failover flow

(1) The ME monitors the state information of the active CE/SCE.

(2) Faults occur in the active CE/SCE.

(3) The ME detects the CE/SCE fault.

(4) The ME sends the same VNE configurations and operation configurations, e.g., static route configuration, routing policies and service policies that the failed CE/SCE was given, and sends the latest state information on the failed CE/SCE to any standby CE/SCE.

(5) The standby CE/SCE joins the VNE including the failed CE/SCE as a new active CE/SCE according to the configurations sent from the ME and starts to operate with the state information sent from the ME.

(6) After recovering from a fault, the failed CE/SCE returns to the iSCP network as a new standby CE/SCE.

In some cases, after fault recovery, the failed CE/SCE may have to return to the iSCP network as an active CE/SCE of the VNE that the failed CE/SCE belonged to previously. Figure I.2 shows another example of the CE/SCE failover flows describing how the CE/SCE fault can be handled in these cases.

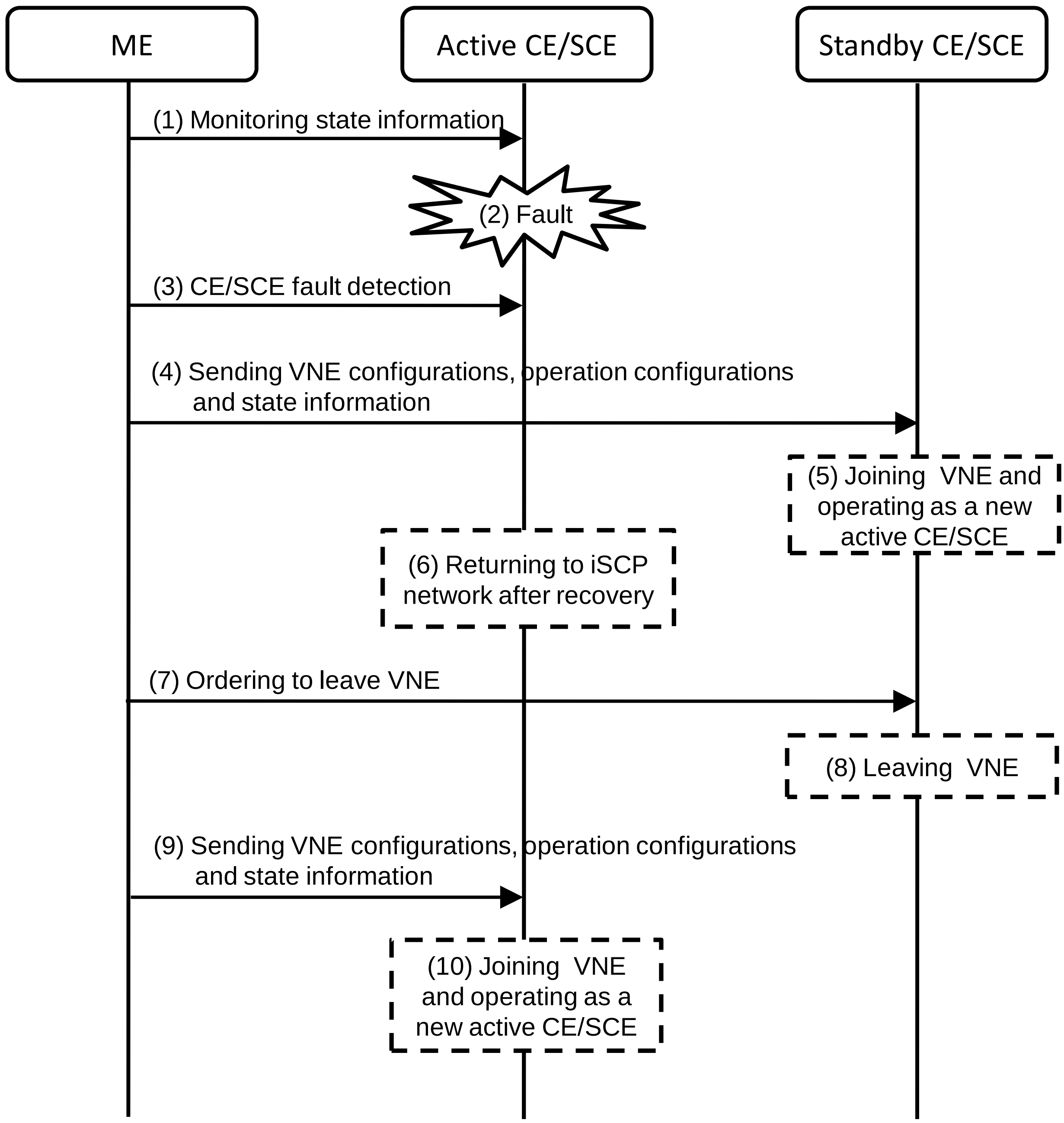

Figure I.2 – Example of CE/SCE failover flow where the failed CE/SCE returns to its original position

(1) The ME monitors the state information of the active CE/SCE.

(2) Faults occur in the active CE/SCE.

(3) The ME detects the CE/SCE fault.

(4) The ME sends the same VNE configurations and operation configurations, e.g., static route configuration, routing policies and service policies that the failed CE/SCE was given, and sends the latest state information on the failed CE/SCE to any standby CE/SCE.

(5) The standby CE/SCE joins the VNE including the failed CE/SCE as a new active CE/SCE according to the configurations sent from the ME and starts to operate with the state information sent from the ME.

(6) After recovering from a fault, the failed CE/SCE returns to the iSCP network.

(7) The ME orders the new active CE/SCE to leave the VNE.

(8) The new active CE/SCE leaves the VNE.

(9) The ME sends the same VNE configurations and operation configurations, e.g., static route configuration, routing policies and service policies that the new active CE/SCE was given, and sends the latest state information on the new active CE/SCE to the recovered CE/SCE.

(10) The recovered CE/SCE joins the VNE as a new active CE/SCE according to the configurations sent from the ME and starts to operate with the state information sent from the ME.

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

[b-ITU-T Y-Sup.11] ITU-T Y-series Recommendations – Supplement 11 (2010), *ITU-T Y.2600 series – 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).*

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, 2013