ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.4493 (11/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Autonomic operations support protocols in the Internet of things

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	**Y.4400-Y.4549**
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

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

Recommendation ITU-T Y.4493

Autonomic operations support protocols in the Internet of things

Summary

Recommendation ITU-T Y.4493 describes autonomic operations support protocols in the Internet of things (IoT) based on the architecture of the IoT specified in Recommendation ITU-T Y.4416, in order to support provisioning of autonomic operation capabilities specified in Recommendation ITU-T Y.4401. Recommendation ITU-T Y.4493 describes the architecture of autonomic operations support protocols in the IoT for: autonomic event management; autonomic control; and autonomic policy management. Possible deployment and relevant use cases of these autonomic operations support protocols in the IoT are described.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.4493	2023-11-29	20	11.1002/1000/15687

Keywords

Autonomic operation, event management, Internet of things, policy management, protocols.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4493

Autonomic operations support protocols in the Internet of things

1 Scope

This Recommendation describes architecture for autonomic operations support protocols, such as autonomic service provisioning and autonomic data operation specified in [ITU-T Y.4401], in the Internet of things (IoT) based on the architecture of the IoT specified in [ITU-T Y.4416]. This Recommendation specifies protocols to support autonomic event management, autonomic control and autonomic policy management based on IoT functional entities (FEs) and referenced points extended in [ITU-T Y.4416] in order to support autonomic operations in the IoT.

This Recommendation includes:

– architecture of autonomic operations support protocols in the IoT;

– autonomic event management support protocol (AEM-SP) in the IoT;

– autonomic control support protocol (AC-SP) in the IoT.

– autonomic policy management support protocol (APM-SP) in the IoT.

The security of autonomic operations support protocols in the IoT specified in this Recommendation is considered, and possible deployment and relevant use cases are described.

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.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

[ITU-T Y.4416] Recommendation ITU-T Y.4416 (2018), *Architecture of the Internet of things based on next generation network evolution*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 Internet of things [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC Autonomic Control

AEM Autonomic Event Management

APM Autonomic Policy Management

DEM Data Event Management

DSA Data Service Adaptation

EAC End-point Access Control

EEM End-point Event Management

FE Functional Entity

ID Identifier

IoT Internet of Things

NGN Next Generation Network

NGNe Next Generation Network evolution

SP Support Protocol

SPA Service Provision Adaptation

TCA Transport Configuration Adaptation

TEM Transport Event Management

5 Conventions

None.

6 Architecture of autonomic operations support protocols

6.1 Overview of the architecture of autonomic operations support protocols

The architecture of autonomic operations support protocols includes the FEs of the IoT architecture specified in [ITU-T Y.4416], the relations of these FEs by using the protocols of supporting autonomic operations in the IoT, and the functions of these protocols in supporting autonomic operations in the IoT.

In this Recommendation, autonomic operations refer to activities related to the set of autonomic capabilities specified in [ITU-T Y.4401], such as autonomic service provisioning, autonomic networking and autonomic data operation.

The architecture of autonomic operations support protocols is illustrated in Figure 6-1. They can be classified as: AEM-SP; AC-SP; or APM-SP.

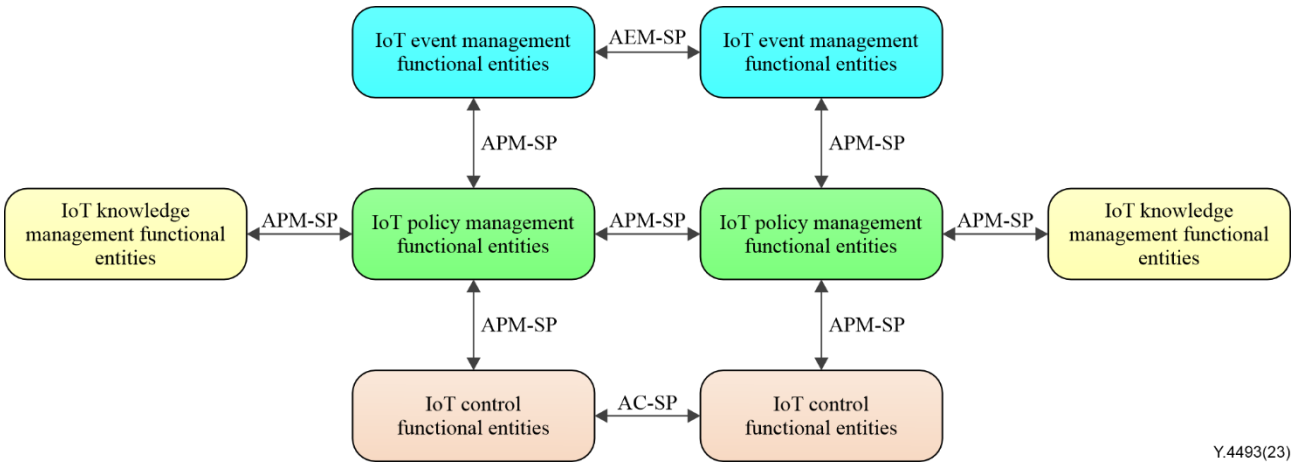

Figure 6-1 – Architecture of autonomic operations support protocols

The AEM-SP is used to implement the reference points among IoT event management FEs. The IoT event management FEs specified in [ITU-T Y.4416] are listed in clause 6.2. The reference points among IoT event management FEs, which include TI-EI-1, DI-EI-1, DI-TI-1, SI-EI-1, SI-TI-1 and SI-DI-1, are also specified in [ITU-T Y.4416].

The AC-SP is used to implement the reference points among IoT control FEs. The IoT control FEs specified in [ITU-T Y.4416] are listed in clause 6.3. The reference points among IoT control FEs, which include TI-EI-2, DI-EI-2, DI-TI-2, SI-EI-2, SI-TI-2 and SI-DI-2, are also specified in [ITU-T Y.4416].

The APM-SP is used to implement three types of reference point. The first type is between IoT event management FEs and IoT policy management FEs. The IoT policy management FEs specified in [ITU-T Y.4416] are listed in clause 6.4. These reference points between IoT event management FEs and IoT policy management FEs, which include EI-EI-1, TI-TI-1, DI-DI-1 and SI-SI-1, are also specified in [ITU-T Y.4416].

The second type of reference point implemented by the APM-SP is between IoT control FEs and IoT policy management FEs. These reference points between IoT control FEs and IoT policy management FEs, which include EI-EI-2, TI-TI-2, DI-DI-2 and SI-SI-2, are specified in [ITU-T Y.4416].

The third type of reference point implemented by the APM-SP is between IoT knowledge management FEs and IoT policy management FEs. The IoT knowledge management FEs specified in [ITU-T Y.4416] are listed in clause 6.4. These reference points between IoT knowledge management FEs and IoT policy management FEs, which include EI-EI-3, TI-TI-3, DI-DI-3 and SI-SI-3, are also specified in [ITU-T Y.4416].

The APM-SP can also be used among distributed implementations of the same type of IoT policy management FEs as illustrated in Figure 6-1, in order to collaborate with IoT policy management in the same functional layer.

NOTE – These three autonomic operations support protocols only implement those reference points that are among or between IoT FEs extended to support IoT capabilities in [ITU-T Y.4416]. These three protocols do not implement all reference point related to the FEs of next generation network (NGN) evolution that are enhanced to support IoT capabilities in [ITU-T Y.4416]. So, specifications of all protocols based on NGN evolution lie outside the scope of this Recommendation.

6.2 Functions of autonomic event management support protocol

The AEM-SP can be used to implement reference points among IoT event management FEs, which include the IoT end-point event management FE (IoT-EEM-FE), IoT transport event management FE (IoT-TEM-FE), IoT data event management FE (IoT-DEM-FE) and IoT service event management

FE (IoT-SEM-FE). All these IoT event management-related FEFEs and their related reference points are specified in [ITU-T Y.4416].

The functions of AEM-SP include:

– collecting events that occurred in different IoT functional layers in order to support cross-layer IoT event capturing;

– collecting events that occurred in distributed implementations of the same type of IoT event management FE in order to support distributed IoT event capturing;

– collaborating events processing with other event management FEs in different IoT functional layers in order to support cross-layer IoT event processing;

– collaborating with events processing among distributed implementations of the same type of IoT event management FEs in order to support distributed IoT event processing.

6.3 Functions of autonomic control support protocol

The AC-SP can be used to implement the reference points among IoT control FEs, which include the IoT end-point access control FE (IoT-EAC-FE), IoT transport configuration adaptation FE (IoT-TCA-FE), IoT data service adaptation FE (IoT-DSA-FE), and IoT service provision adaptation FE (IoT-SPA-FE). All these IoT control-related FEs and their related reference points are specified in [ITU-T Y.4416].

The functions of AC-SP include:

– collaborating IoT configuration and adaptation control with other IoT control FEs in different IoT functional layers in order to support cross-layer control of IoT autonomic operations and initiate possible autonomic operations across different functional layers of the IoT;

– collaborating with IoT configuration and adaptation control among distributed implementations of one type of IoT control FEs in order to support distributed control of IoT autonomic operations and initiate possible autonomic operations within the same functional layers of the IoT.

6.4 Functions of autonomic policy management support protocol

The (APM-SP can be used to implement reference points of IoT policy management FEs in the same functional layer, which include the IoT end-point policy enforcement FE (IoT-EPE-FE), IoT transport policy enforcement FE (IoT-TPE-FE), IoT data policy enforcement FE (IoT-DPE-FE) and IoT service policy enforcement FE (IoT-SPE-FE). All these IoT policy management FEs and their related reference points are specified in [ITU-T Y.4416].

The APM-SP can be used to implement reference points between IoT event management FEs and IoT policy management FEs, in order to support the functions of policy-enforced IoT event management.

The APM-SP can be used to implement reference points between IoT control FEs and IoT policy management FEs, in order to support the functions of policy-enforced IoT control.

The APM-SP can be used to implement reference points between IoT policy management FEs and IoT knowledge management FEs, in order to support the functions of controlling new knowledge learning in the IoT knowledge management FEs and updating policies based on the new knowledge.

The IoT knowledge management FEs include the IoT end-point knowledge management FE (IoT-EKM-FE), IoT transport knowledge management FE (IoT-TKM-FE), IoT data knowledge management FE (IoT-DKM-FE), and IoT service knowledge management FE (IoT-SKM-FE). All these IoT knowledge management FEs are specified in [ITU-T Y.4416].

The functions of the APM-SP include:

– controlling and obtaining new knowledge learned in the IoT knowledge management FEs in order to update intelligent policies to support IoT autonomic operations in some unknown environments, such as an IoT device moving to a new operating environment;
– collaborating with IoT policy management among distributed implementations of one type of IoT policy enforcement FEs in order to support distributed policy enforcement on the IoT autonomic operations;
– collaborating with IoT event management FEs in order to support the functions of IoT autonomic operations with the help of policy-enforced IoT event management capabilities;
– collaborating with IoT control FEs in order to support the functions of IoT autonomic operations with the help of policy-enforced IoT control capabilities.

NOTE – The cross-layer policy management should be under control of human operators. The function of cross-layer policy management lies outside the scope of this Recommendation.

7 Autonomic event management support protocol

7.1 Scope of autonomic event management support protocol

The scope of the AEM-SP includes the two following aspects:

– exchange of event management messages among IoT event management FEs of different functional layers, in order to coordinate event management of different functional layers and support event capturing and processing across different functional layers of the IoT;
– exchange of event management messages among IoT event management FEs within the same functional layers, in order to coordinate event management of the same functional layers and support event capturing and processing among the networked nodes of the IoT.

The scope of the AEM-SP is illustrated in Figure 7-1. The IoT event management FEs illustrated in Figure 7-1, such as EI-1: IoT-EEM-FE, TI-1: IoT-TEM-FE, DI-1: IoT-DEM-FE and SI-1: IoT-SEM-FE, are specified in [ITU-T Y.4416].

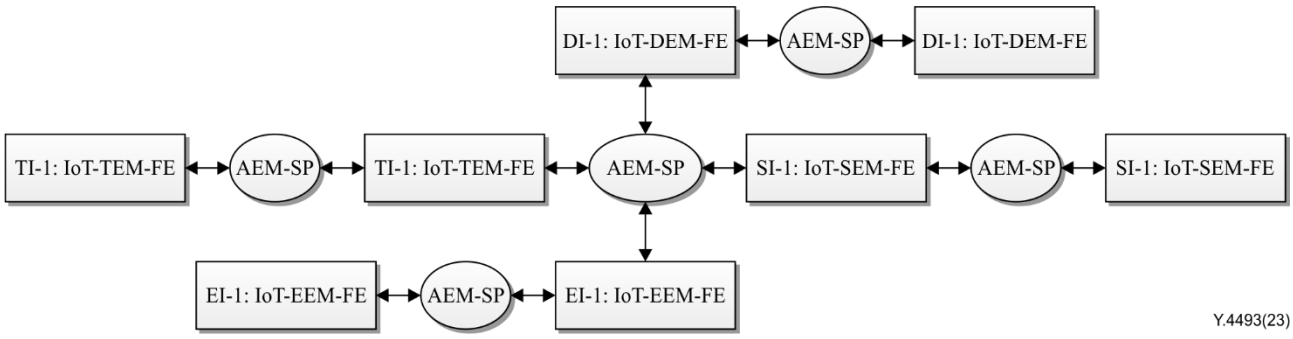

Figure 7-1 – Scope of autonomic event management support protocol

7.2 Features of autonomic event management support protocol

The AEM-SP includes the following features:

– the AEM-SP is a group protocol (as illustrated in Figure 7-1) that can send messages to several IoT event management FEs that belong to one group;
– different AEM-SP groups can be established to manage different types of events.

7.3 Message structure of autonomic event management support protocol

The message structure of the AEM-SP consists of a message head and message body. The message head consists of an AEM-SP identifier (AEM-SP-ID, 8 bits), protocol version number (8 bits), and message length (16 bits). The message body consists of several AEM-SP fields. Each field consists

of field type (8 bits), field length (16 bits), and field value that can be specified by different types of fields. The message structure of the AEM-SP is illustrated in Figure 7-2.

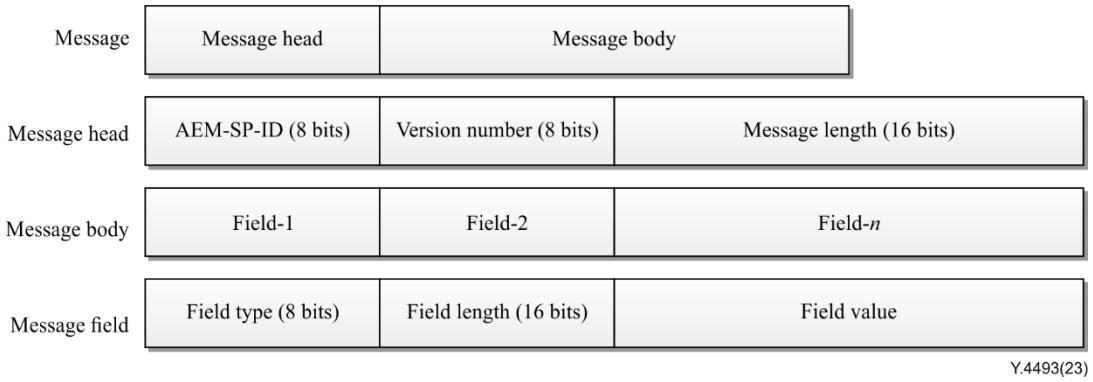

Figure 7-2 – Message structure of autonomic event management support protocol

The fields of an AEM-SP message are used to realize the functionalities of AEM-SP. Based on the scope and features of the AEM-SP, the field types of AEM-SP are divided into two categories: AEM-SP group management and event management.

7.3.1 Basic fields of autonomic event management support protocol group management category

The basic fields of the AEM-SP group management category include the group address, group ID, AEM-SP-ID, group security level, group manager ID, group manager address and group access control data.

NOTE 1 – Any type of existing or self-defined group address, either in the network functional or application functional layer, can be used.

NOTE 2 – The group security level can be used to introduce possible security-related capabilities into the autonomic operation support protocol in order to satisfy the application requirements on this aspect. This Recommendation does not specify the field type in detail.

7.3.2 Basic fields of event management category

The basic fields of the event management category include event initiator ID, event ID, event sender ID, event description, and event data.

7.4 Functionalities of autonomic event management support protocol

The functionalities of the AEM-SP can be classified into those for group management and event management, based on its scope and features.

NOTE 1 – The functionalities of AEM-SP specified in this clause relate to message exchange among IoT event management FEs, which are different from the IoT event management functions specified in the IoT event management FEs. IoT event management FEs are specified in [ITU-T Y.4416].

NOTE 2 – The AEM-SP is specified as a self-containment protocol whose specifications do not depend on any existing protocol. The implementation of the AEM-SP can rely on that of existing protocols to multicast AEM-SP messages within the event management group. The mechanisms or methods of implementing the AEM-SP lie outside the scope of this Recommendation.

7.4.1 Functionalities of autonomic event management support protocol group management

The functionalities of AEM-SP group management include those of assigning group managers, updating group manager, adding group members, updating group members and multicasting event messages within the group.

1) Assigning group managers

Group managers are entities of the AEM-SP that can establish and update its group, and store and update group information. Group managers include one active and several backup types.

During the initiation stage of the AEM-SP, an active group manager and at least one backup manager are assigned. Group managers should perform the following operations:

– the active group manager should broadcast an announcement of the group address periodically;
– the active group manager should listen for new member messages to the group address and prepare to adopt new members to join this group;
– the active group manager should be able to authenticate new group members when required based on the requirements of a specified security level;
– the active group manager should send heartbeat messages periodically to all group members to check whether they are active;
– backup group managers should listen for messages sent by active group managers and prepare to act as an active group manager when the current one has not been in active.

2) Updating group manager

An updating group manager functionality changes the configuration of the active or backup group managers, and replaces an active with a backup group manager. Updating the configuration of the active or backup group managers belongs to the management functionality that can be implemented by the management interfaces of the AEM-SP. The replacement of the active group manager is an AEM-SP functionality, which should perform the following operations:

– backup group managers should listen for both announcements and heartbeat messages sent by active group managers;
– backup group managers should compete for a new active group manager when neither announcements nor heartbeat messages have been received for a period of time;
– a competent backup group manager should take over the role of active group manager and perform all its operations when necessary.

3) Adding group members

Adding group members involves listening for new member messages to the group address, authenticating new group members when necessary, and updating group information when a new group member has been adopted. The following operations should be supported to provide the functionality of adding group members:

– the new AEM-SP entity should receive the announcement broadcast by the active group manager;
– the new AEM-SP entity should send a new member message from the group address;
– the new AEM-SP entity should provide data that can be authenticated by the active group manager when required based on the requirements of a specified security level.

4) Updating group members

Updating group members involves checking the active status of all group members, deleting those that are inactive and updating group information accordingly. In order to provide the functionality to update group members, the following operations should be supported:

– the active group manager should send heartbeat messages periodically to all group members to check whether they are active;
– group members should receive heartbeat messages in a timely fashion;
– group members should respond to heartbeat messages received in a timely fashion.

5) Multicasting event messages within the group

Multicasting messages within the group involves sending event management messages to all group members based on the information stored by the active group manager. The following operations should be supported to provide the functionality of multicasting messages within the group:

– the active group manager should receive event management messages at all group addresses belonging to this group;

– the active group manager should transfer event management messages to all group addresses within the group except for those from which they have been received.

7.4.2 Functionalities of autonomic event management support protocol event management

The functionalities of AEM-SP event management include those of initiating event messages, receiving event messages, transferring event messages, binding events to groups and unbinding events from groups.

1) Initiating event messages

Initiating event messages involves their preparation and dispatch to relevant groups by an AEM-SP entity. In order to support this functionality, the following operations should be performed:

– the AEM-SP entity should gather event information and encode it into event messages;

– the AEM-SP entity should identify the types of event and select the group to receive event messages based on predefined event management policies and machine-learned knowledge of event management;

– the AEM-SP entity should send the event messages to the addresses of the groups selected.

2) Receiving event messages

Receiving event messages involves identification of events in messages and their delivery to the corresponding management entities. Receiving event messages also involves identification of groups bound by the event type in event messages and determination of whether it is necessary to transfer such messages to groups other than those already receiving them, when the receiving AEM-SP entity acts as an active group manager. The following operations should be performed to support the functionality of receiving event messages in the AEM-SP entity:

– the AEM-SP entity identifies the events in the messages received and delivers them to the corresponding management entities based on predefined event management policies and machine-learned knowledge of event management;

– active group managers identify the groups bound by the event type in these event messages and decide whether it is necessary to transfer the event messages to groups other than those already receiving them.

3) Transferring event messages

Transferring event messages involves checking the relevant groups in which there is no event message that is similar to those received and transferring the received event messages to these groups. The following operations should be performed in order to support the functionality of transferring event messages:

– the active group manager that has received event messages should list all groups that are bound to the events in the event messages received;

– the active group manager that has received event messages should check all groups that are bound to the events in the received event messages and identify all groups in which there is no event message that is similar to those received;

– the active group manager that has received event messages should transfer the event messages to the groups that are bound to the events in the event messages and check there is no similar event message in these groups.

4) Binding events to groups

Binding events to groups involves binding event types to the event management groups in AEM-SP. The following operations should be performed by AEM-SP entities in order to support the functionalities of binding events to event management groups:

– the AEM-SP entity that needs to bind one or several types of events to some event management groups should encode all necessary data related to binding the events to groups in a group binding message;

– the AEM-SP entity that needs to bind one or more types of events to some event management groups should send a group binding message to the groups bound by the event or events;

– the active group manager that has received a group binding message should initiate an event type and event group management table if none exists and add all binding relations in a group binding message to the table;

– an active group manager that has received a group binding message should update the event type and event group management table if already established, by adding all the binding relations in the group binding message to the table.

5) Unbinding events from groups

Unbinding events from groups involves unbinding event types from event management groups in the AEM-SP. The following operations should be performed by AEM-SP entities in order to support the functionalities of unbinding events from event management groups:

– the AEM-SP entity that needs to unbind one or several types of events from some event management groups should encode all necessary data related to unbinding the events from groups in a group unbinding message;

– the AEM-SP entity that needs to unbind one or more types of events from some event management groups should send a group unbinding message to the groups unbound from the event or events;

– an active group manager that has received a group unbinding message should update the control type and control coordination group management table. If the table does not exist, it should be created. The manager should then delete all the binding relations in the group binding message from the table.

8 Autonomic control support protocol

8.1 Scope of autonomic control support protocol

The scope of the AC-SP includes the two following aspects:

– exchange of control messages among IoT control FEs of different functional layers, in order to coordinate control operations of different functional layers and initiate possible autonomic operations across different functional layers of the IoT;

– exchange of control message among IoT control FEs within the same functional layers, in order to coordinate control operations of the same functional layers and initiate possible autonomic operations within the same functional layers of the IoT.

The scope of the AC-SP is illustrated in Figure 8-1. The IoT control FEs illustrated in Figure 8-1, such as EI-4: IoT-EAC-FE, TI-4: IoT-TCA-FE, DI-4: IoT-DSA-FE and SI-4: IoT-SPA-FE, are specified in [ITU-T Y.4416].

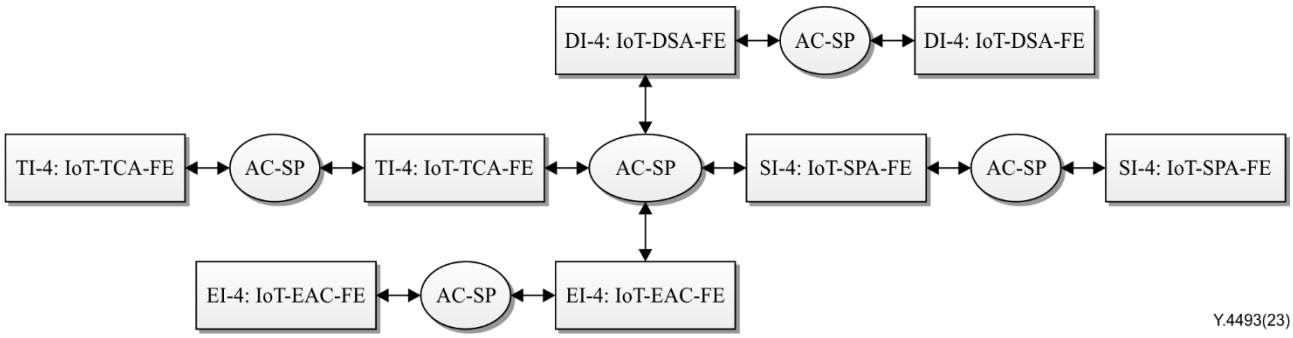

Figure 8-1 – Scope of autonomic control support protocol

8.2 Features of autonomic control support protocol

The AC-SP includes the two following features:

– the AC-SP is a group protocol (as illustrated in Figure 8-1) that can send messages to several IoT control FEs that belong to one group;

– different AC-SP groups can be established to control different types of operations.

8.3 Message structure of autonomic control support protocol

The message structure of the AC-SP consists of a message head and message body. The message head consists of the AC-SP-ID (8 bits), protocol version number (8 bits), and message length (16 bits). The message body consists of several AC-SP fields. Each field consists of field type (8 bits), field length (16 bits), and field value that can be specified by different types of fields. The message structure of AC-SP is illustrated in Figure 8-2.

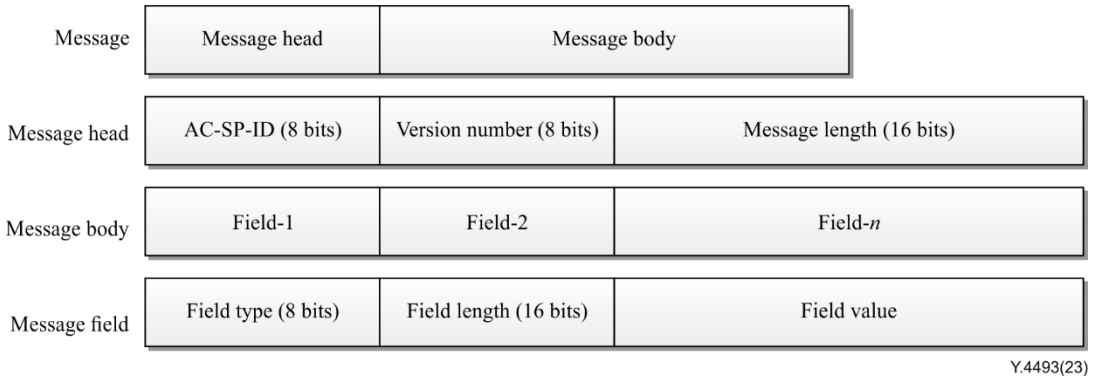

Figure 8-2 – Message structure of autonomic control support protocol

The fields of an AC-SP message are used to realize the functionalities of the AC-SP. Based on the scope and features of the AC-SP, the field types of AC-SP are divided into following categories for: AC-SP group management; single-layer control coordination; and cross-layer control coordination.

8.3.1 Basic fields of autonomic control support protocol group management category

The basic fields of the AC-SP group management category include group address, group ID, AC-SP-ID, group security level, cross-layer group indication, group manager ID, group manager address and group access control data.

NOTE 1 – Any type of existing or self-defined group address, either in network functional layer or in application functional layer, can be used.

NOTE 2 – The group security level can be used to introduce possible security-related capabilities into the autonomic operation support protocol in order to satisfy the application requirements on this aspect. This Recommendation does not specify the field type in detail.

8.3.2 Basic fields of single-layer control coordination category

The basic fields of the single-layer control coordination category include control coordinator ID, control classifier (such as end-point, transport, data and service), relevant-event ID, and control data.

NOTE – The control data include the text describing the purposes and features of the control, as well as the rules enforced by the control.

8.3.3 Basic fields of cross-layer control coordination category

The basic fields of the cross-layer control coordination category include control coordinator ID, coordinator-layer ID, relevant control entity ID, relevant control layer ID, control classifier (such as end-point, transport, data and service), relevant-event ID, and control data.

NOTE – The control data include the text describing the purposes and features of the control, as well as the rules enforced by the control.

8.4 Functionalities of autonomic control support protocol

The functionalities of the AC-SP can be classified into those for group management and control coordination, based on its scope and features.

NOTE – The AC-SP is specified as a self-containment protocol whose specifications do not depend on any existing protocol. The implementation of the AC-SP can rely on that of existing protocols to multicast AC-SP messages within the control group. The mechanisms or methods of implementing the AC-SP lie outside the scope of this Recommendation.

8.4.1 Functionalities of autonomic control support protocol group management

The functionalities of AC-SP group management include those of assigning group managers, updating group manager, adding group members, updating group members, and multicasting control coordination messages within the group.

1) Assigning group managers

   Group managers are entities of the AC-SP that can establish and update its group, and store and update group information. Group managers include one active and several backup types.

   During the initiation stage of the AC-SP, an active group manager and at least one backup manager are assigned. Group managers should perform the following operations:

   – the active group manager should broadcast an announcement of the group address periodically;
   – the active group manager should listen for new member messages to the group address and prepare to adopt new members to join this group;
   – the active group manager should be able to authenticate new group members when required based on the requirements of a specified security level;
   – the active group manager should send heartbeat messages periodically to all group members to check whether they are active;
   – backup group managers should listen for messages sent by active group managers and prepare to take over the role of active group manager when the current one has not been in active.

2) Updating group manager

   An updating group manager functionality changes the configuration of the active or backup group managers, and replaces the active group manager with a backup group manager. Updating the configuration of the active or backup group managers belongs to the management functionality that can be implemented by the management interfaces of the AC-SP. The replacement of the active group manager is an AC-SP functionality, which should perform the following operations:

– backup group managers should listen for both announcements and heartbeat messages sent by active group managers;
– backup group managers should compete for a new active group manager when neither announcements nor heartbeat messages have been received for a period of time;
– a competent backup group manager should take over the role of the active group manager and perform all its operations when necessary.

3) Adding group members

Adding group members involves listening for new member messages to the group address, authenticating new group members when necessary, and updating group information when a new group member has been adopted. The following operations should be supported to provide the functionality of adding group members:

– the new AC-SP entity should receive the announcement broadcast by the active group manager;
– the new AC-SP entity should send the new-member message from the group address;
– the new AC-SP entity should provide the authentic data that can be authenticated by the active group manager when required based on the requirements of a specified security level.

4) Updating group members

Updating group members involves checking the active status of all group members, deleting those that are inactive, and updating group information accordingly. In order to provide the functionality to update group members, the following operations should be supported:

– the active group manager should send heartbeat messages periodically to all the group members to check whether they are active;
– group members should receive heartbeat messages in a timely fashion;
– group members should respond to the heartbeat messages received in a timely fashion.

5) Multicasting control coordination messages within the group

Multicasting messages within the group involves sending control coordination messages to all group members based on the information stored by the active group manager. The following operations should be supported to provide the functionality of multicasting messages within the group:

– the active group manager should receive control coordination messages at all group addresses belonging to this group;
– the active group manager should transfer control coordination messages to all group addresses within the group except for those from which they have been received.

8.4.2 Functionalities of autonomic control support protocol control coordination

The functionalities of AC-SP control coordination include those of initiating control coordination messages, receiving control coordination messages, transferring control coordination messages, binding controls to groups and unbinding controls from groups.

1) Initiating control coordination messages

Initiating control coordination messages involves their preparation and dispatch to relevant groups by an AC-SP entity. In order to support this functionality, the following operations should be performed:

– the AC-SP entity should gather control information and encode it into control coordination messages;

– the AC-SP entity should identify the types of control and select the group to receive control coordination messages based on predefined control coordination policies and machine-learned knowledge of control coordination;
– the AC-SP entity should send the control coordination messages to the addresses of the groups selected.

2) Receiving control coordination messages

Receiving control coordination messages involves identification of controls in messages and their delivery to the corresponding control-related entities. Receiving control coordination messages also involves identification of groups bound by the control type in control coordination messages and determination of whether it is necessary to transfer such messages to groups other than those already receiving them, when the receiving AC-SP entity acts as an active group manager. The following operations should be performed to support the functionality of receiving control coordination messages in the AC-SP entity:

– the AC-SP entity identifies the controls in the messages received and delivers them to the corresponding control-related entities based on predefined control coordination policies and machine-learned knowledge of control coordination;
– the active group managers identify the groups bound by the control type in these control coordination messages and decide whether it is necessary to transfer the control coordination messages to groups other than those already receiving them.

3) Transferring control coordination messages

Transferring control coordination messages involves checking the relevant groups in which there is no control coordination message that is similar to those received and transferring the received control coordination messages to these groups. The following operations should be performed in order to support the functionality of transferring control coordination messages:

– the active group manager that has received control coordination messages should list all groups that are bound to the controls in the control coordination messages received;
– the active group manager that has received control coordination messages should check all groups that are bound to the controls in the received control coordination messages and identify all groups in which there is no control coordination message that is similar to those received;
– the active group manager that has received control coordination messages should transfer them to the groups that are bound to the controls in the control coordination messages and check there is no similar control coordination message in these groups.

4) Binding controls to groups

Binding controls to groups involves binding control types to the control coordination groups in the AC-SP. The following operations should be performed by AC-SP entities in order to support the functionalities of binding controls to control coordination groups:

– the AC-SP entity that needs to bind one or several types of control to some control coordination groups should encode all necessary data related to binding the controls to groups in a group binding message;
– the AC-SP entity that needs to bind one or more types of control to some control coordination groups should send a group binding message to the groups bound by the control or controls;
– the active group manager that has received a group binding message should initiate a control type and control coordination group management table if none exists and add all the binding relations in the group binding message to the table;

– the active group manager that has received a group binding message should update the control type and control coordination group management table if already established, by adding all the binding relations in the group binding message to the table.

5) Unbinding controls from groups

Unbinding controls from groups involves unbinding control types from control coordination groups in the AC-SP. The following operations should be performed by AC-SP entities in order to support the functionalities of unbinding controls from control coordination groups:

– the AC-SP entity that needs to unbind one or several types of control from some control coordination groups should encode all necessary data related to unbinding the controls from groups in a group unbinding message;

– the AC-SP entity that needs to unbind one or more types of control from some control coordination groups should send a group unbinding message to the groups unbound from the control or controls;

– an active group manager that has received a group unbinding message should update the control type and control coordination group management table if none exists, by deleting all the binding relations in the group unbinding message from the table.

9 Autonomic policy management support protocol

9.1 Scope of autonomic policy management support protocol

The APM-SP is in the centre of the autonomic operations support protocol as illustrated in Figure 6-1. The scope of the APM-SP can be classified into two parts: implementation of reference points among the policy enforcement FEs that are specified in [ITU-T Y.4416]; and implementation of reference points between the policy enforcement FEs and other FEs that are specified in [ITU-T Y.4416]. The scope of the first part of the APM-SP includes the two following:

– exchange of policy enforcement messages among IoT policy enforcement FEs of different functional layers, in order to coordinate policy enforcement operations of different functional layers and initiate possible policy management operations across different functional layers of the IoT. The cross-layer policy management should be under control of human operations through predefined policies and necessary human intervention;

– exchange of policy enforcement messages among IoT policy enforcement FEs within the same functional layers, in order to coordinate policy enforcement operations of the same functional layers and initiate autonomic operations among the networked nodes of the IoT.

The scope of the first part of the APM-SP is illustrated in Figure 9-1. The IoT policy enforcement FEs illustrated in Figure 9-1, such as EI-2: IoT-EPE-FE, TI-2: IoT-TPE-FE, DI-2: IoT-DPE-FE and SI-2: IoT-SPE-FE, are specified in [ITU-T Y.4416].

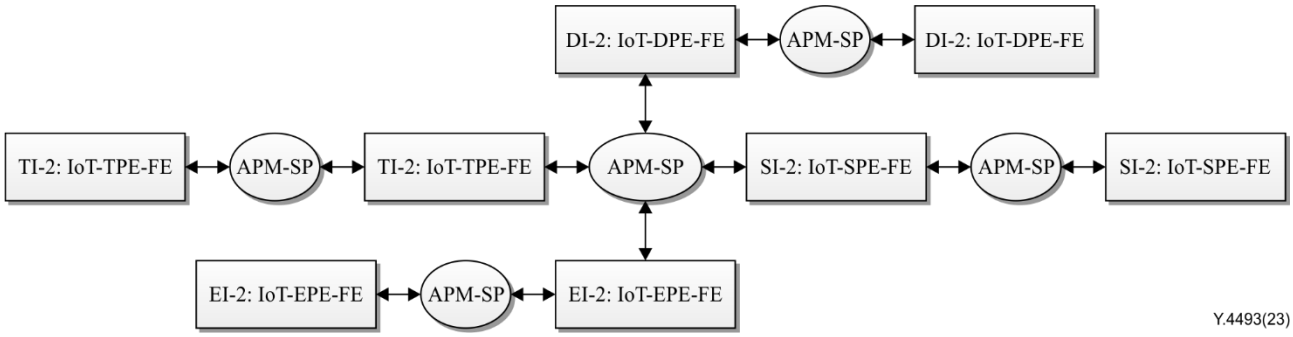

Figure 9-1 – Scope of autonomic policy management support protocol – part I

The scope of the second part of the APM-SP includes the three following aspects:

– exchange policy enforcement messages between IoT policy enforcement FEs and IoT knowledge management FEs within the same functional layer, in order to coordinate policy enforcement operations on IoT knowledge management in the same functional layer and update IoT policies in the IoT policy enforcement FEs;

– exchange policy enforcement messages between IoT policy enforcement FEs and IoT event management FEs within the same functional layer, in order to coordinate policy enforcement operations on IoT event management in the same functional layer, and make decision on initiating and controlling autonomic operations;

– exchange policy enforcement messages between IoT policy enforcement FEs and IoT control FEs within the same functional layer, in order to coordinate policy enforcement operations on IoT control in the same functional layer, and decide on initiating and controlling autonomic operations.

The scope of the second part of the APM-SP is illustrated in Figure 9-2.

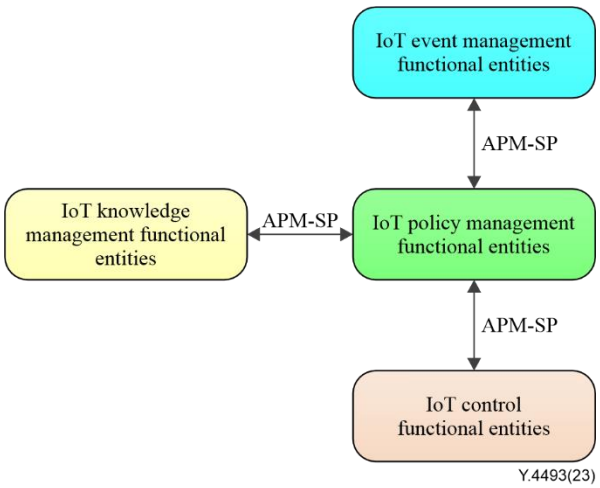

Figure 9-2 – Scope of autonomic policy management support protocol – part II

9.2 Features of autonomic policy management support protocol

The APM-SP includes the following features:

– the APM-SP is a group protocol (as illustrated in Figure 9-1) when it is used among IoT policy enforcement entities that can send messages to several IoT policy enforcement FEs that belong to one group;

– different APM-SP groups can be established to manage different types of policies;

– the APM-SP is a peer-to-peer protocol when it is used for interacting between the IoT policy enforcement entities and other FEs, as illustrated in Figure 9-2.

9.3 Message structure of autonomic policy management support protocol

The message structure of the APM-SP consists of a message head and message body. The message head consists of the APM-SP-ID (8 bits), protocol version number (8 bits) and message length (16 bits). The message body consists of several APM-SP fields. Each field consists of field type (8 bits), field length (16 bits), and field value that can be specified by different types of fields. The message structure of the APM-SP is illustrated in Figure 9-3.

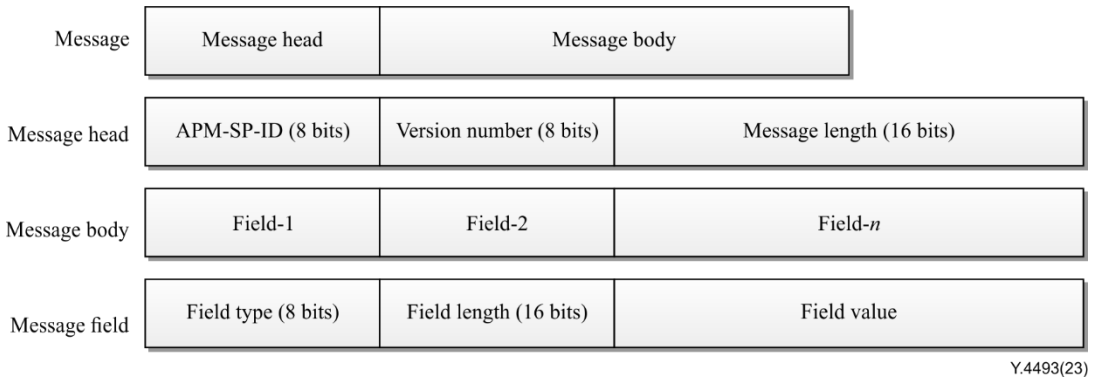

Figure 9-3 – Message structure of autonomic policy management support protocol

The fields of an APM-SP message are used to realize the functionalities of APM-SP. According to its scope and features, the field types of the APM-SP are divided into following categories for: APM-SP group management; policy management; policy-enforced knowledge learning; policy-enforced event management; and policy-enforced control.

9.3.1 Basic fields of autonomic policy management support protocol group management category

The basic fields of the APM-SP group management category include group address, group ID, APM-SP-ID, group security level, cross-layer group indication, group manager ID, group manager address, and group access control data.

NOTE 1 – Any type of existing or self-defined group address, either in network functional layer or in application functional layer, can be used.

NOTE 2 – The group security level can be used to introduce possible security-related capabilities into the autonomic operation support protocol in order to satisfy the application requirements on this aspect. This Recommendation does not specify the field type in detail.

9.3.2 Basic fields of policy management category

The basic fields of the policy management category include policy query, policy validating, policy adding, policy deleting, and policy modifying.

9.3.3 Basic fields of policy-enforced knowledge learning category

The basic fields of the policy-enforced knowledge learning category include rule-based knowledge check request, rule-based knowledge check response, learning rule validating, learning rule adding, learning rule deleting, and learning rule modifying.

9.3.4 Basic fields of policy-enforced event management category

The basic fields of the policy-enforced event management category include rule-based event check request, rule-based event check response, rule-based event sending, rule-based event data, and rule-violated event data.

9.3.5 Basic fields of policy-enforced control category

The basic fields of the policy-enforced control category include rule-based control check request, rule-based control check response, rule-based control initiation, rule-based control data, and rule-violated control data.

9.4 Functionalities of autonomic policy management support protocol

The functionalities of the APM-SP can be classified into those for group management and policy enforcement, based on its scope and features.

NOTE – The functionalities of APM-SP specified in this clause are related to the message exchange among the IoT policy enforcement FEs, which are different from the IoT policy enforcement functions specified in the IoT policy enforcement FEs. The IoT policy enforcement FEs had been specified in [ITU-T Y.4416].

9.4.1 Functionalities of autonomic policy management support protocol group management

The functionalities of APM-SP group management include those of assigning group managers, updating group manager, adding group members, updating group members, and multicasting policy enforcement messages within the group.

1) Assigning group managers

Group managers are entities of the APM-SP that can establish and update its group, and store and update group information. Group managers include one active and several backup types.

During the initiation stage of the APM-SP, an active group manager and assign at least one backup manager are assigned. Group managers should perform the following operations:

– the active group manager should broadcast an announcement of the group address periodically;

– the active group manager should listen for new member messages to the group address and prepare to adopt new members to join this group;

– the active group manager should be able to authenticate new group members when required based on the requirements of a specified security level;

– the active group manager should send heartbeat messages periodically to all group members to check whether they are active;

– backup group managers should listen for messages sent by active group managers and prepare to take over the role of active group manager when the current one has not been in active.

2) Updating group manager

An updating group manager functionality changes the configuration of the active or backup group managers, and replaces the active group manager with a backup group manager. Updating the configuration of the active or backup group managers belongs to the management functionality that can be implemented by the management interfaces of the APM-SP. The replacement of the active group manager is an APM-SP functionality, which should perform the following operations:

– backup group managers should listen for both announcements and heartbeat messages sent by active group managers;

– backup group managers should compete for a new active group manager when neither announcements nor heartbeat messages have been received for a period of time;

– a competent backup group manager should take over the role of the active group manager and perform all its operations when necessary.

3) Adding group members

Adding group members involves listening for new member messages to the group address, authenticating new group members when necessary, and updating group information when a new group member has been adopted. The following operations should be supported to provide the functionality of adding group members:

– the new APM-SP entity should receive the announcement broadcast by the active group manager;

– the new APM-SP entity should send the new-member message from the group address;

– the new APM-SP entity should provide the authentic data that can be authenticated by the active group manager when required based on the requirements of a specified security level.

4) Updating group members

Updating group members involves checking the active status of all group members, deleting those that are inactive, and updating group information accordingly. In order to provide the functionality to update group members, the following operations should be supported:

– the active group manager should send heartbeat messages periodically to all group members to check whether they are active;

– group members should receive heartbeat messages in a timely fashion;

– group members should respond to heartbeat messages received in a timely fashion.

5) Multicasting policy enforcement messages within the group

Multicasting messages within the group involves sending policy enforcement messages to all group members based on the information stored by the active group manager. The following operations should be supported to provide the functionality of multicasting messages within the group:

– the active group manager should receive policy enforcement messages at all group addresses belonging to this group;

– the active group manager should transfer policy enforcement messages to all group addresses within the group except for those from which they have been received.

9.4.2 Functionalities of autonomic policy management support protocol policy enforcement

The functionalities of APM-SP policy enforcement include those of initiating policy enforcement messages, receiving policy enforcement messages, transferring policy enforcement messages, binding policy enforcement to groups, and unbinding policy enforcement from groups.

1) Initiating policy enforcement messages

Initiating policy enforcement messages involves their preparation and dispatch to relevant groups by an APM-SP entity. In order to support this functionality, the following operations should be performed:

– the APM-SP entity should gather policy enforcement information and encode it into policy enforcement messages;

– the APM-SP entity should identify the types of policy enforcement and select the group to receive policy enforcement messages based on human-determined policies;

– the APM-SP entity should send the policy enforcement messages to the addresses of groups selected.

2) Receiving policy enforcement messages

Receiving policy enforcement messages involves identification of policy enforcements in messages and their delivery to the corresponding policy enforcement entities. Receiving policy enforcement messages also involves identification of groups bound by the policy enforcement type in policy enforcement messages and determination of whether it is necessary to transfer such messages to groups other than those already receiving them, when the receiving APM-SP entity acts as an active group manager. The following operations should be performed to support the functionality of receiving policy enforcement messages in the APM-SP entity:

– the APM-SP entity identifies the policy enforcements in the messages received and delivers them to the corresponding policy enforcement entities based on human-determined policies;

– the active group managers identify the groups bound by the policy enforcement type in these policy enforcement messages and decide whether it is necessary to transfer the policy enforcement messages to groups other than those already receiving them.

3) Transferring policy enforcement messages

Transferring policy enforcement messages involves checking the relevant groups in which there is no policy enforcement message that is similar to those received and transferring the received policy enforcement messages to these groups. The following operations should be performed in order to support the functionality of transferring policy enforcement messages:

– the active group manager that has received policy enforcement messages should list all groups that are bound to the policy enforcements in the policy enforcement messages received;

– the active group manager that has received policy enforcement messages should check all groups that are bound to the policy enforcements in the received policy enforcement messages and identify all groups in which there is no policy enforcement message that is similar to those received;

– the active group manager that has received policy enforcement messages should transfer the policy enforcement messages to the groups that are bound to the policy enforcements in the policy enforcement messages and check there is no similar policy enforcement message in these groups.

4) Binding policy enforcements to groups

Binding policy enforcements to groups involves binding policy enforcement types to the policy enforcement management groups in APM-SP. The following operations should be performed by APM-SP entities in order to support the functionalities of binding policy enforcements to policy enforcement groups:

– the APM-SP entity that needs to bind one or several types of policy enforcement to some policy enforcement groups should encode all necessary data related to binding the policy enforcements to groups in a group binding message;

– the APM-SP entity that needs to bind one or more types of policy enforcement to some policy enforcement groups should send a group binding message to the groups bound by the policy enforcement or policy enforcements;

– the active group manager that has received a group binding message should initiate a policy enforcement type and policy enforcement group management table if none exists and add all the binding relations in the group binding message to the table;

– the active group manager that has received a group binding message should update the policy enforcement type and policy enforcement group management table if already established, by adding all the binding relations in the group binding message to the table.

5) Unbinding policy enforcements from groups

Unbinding policy enforcements from groups involves unbinding policy enforcement types from policy enforcement groups in the APM-SP. The following operations should be performed by APM-SP entities in order to support the functionalities of unbinding policy enforcements from policy enforcement groups:

– the APM-SP entity that needs to unbind one or several types of policy enforcement from some policy enforcement groups should encode all necessary data related to unbinding the policy enforcements from groups in a group unbinding message;

– the APM-SP entity that needs to unbind one or more types of policy enforcement from some policy enforcement groups should send a group unbinding message to the groups unbound from the policy enforcement or policy enforcements;

– an active group manager that has received a group unbinding message should update the policy enforcement type and policy enforcement group management table if none exists, by deleting all the binding relations in the group unbinding message from the table.

10 Security considerations

Security issues have been considered thoroughly in this Recommendation, such as determination of group security level, specification of authenticating a new group member of autonomic operation support protocols and specification of the message structure of cross-layer control coordination.

1) Determination of group security level. The group security level is determined in each message structure of the AEM-SP, AC-SP and APM-SP. The group security level can be used to introduce possible security-related capabilities into autonomic operation support protocols in order to satisfy the security requirements of specific applications.

2) Specification of authentication. In the functionalities of each of the AEM-SP group management protocol, AC-SP group management protocol and APM-SP group management protocol, the active group manager has been assigned a capability to authenticate new group members based on the requirements of a specified security level. The capability can be used to prevent illegal actors from attacking these autonomic operation support protocols.

3) Specification of message structure of cross-layer control coordination. In the message structure of the AC-SP, the basic fields of the cross-layer control coordination category have been specified to include control coordinator ID, coordinator-layer ID, relevant control entity ID, relevant control layer ID, control classifier (such as end-point, transport, data and service), relevant-event ID and control data. This message structure can be used to prevent possible attack across functional layers.

Appendix I

Possible deployment of autonomic operations support protocols

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

Autonomic operations support protocols can be used to implement the reference points specified in [ITU-T Y.4416]. One use case of autonomic communication is used to illustrate possible deployment of autonomic operations support protocols specified in this Recommendation.

I.1 A use case of autonomic communications between IoT devices

When an IoT device identifies the occurrence of a critical event based on predefined policies, it needs to automatically initiate a communication to its controller, such as another IoT device or an IoT gateway, to report the event. It is a typical use case of autonomic communication between IoT devices. This use case is shown in Figure I.1.

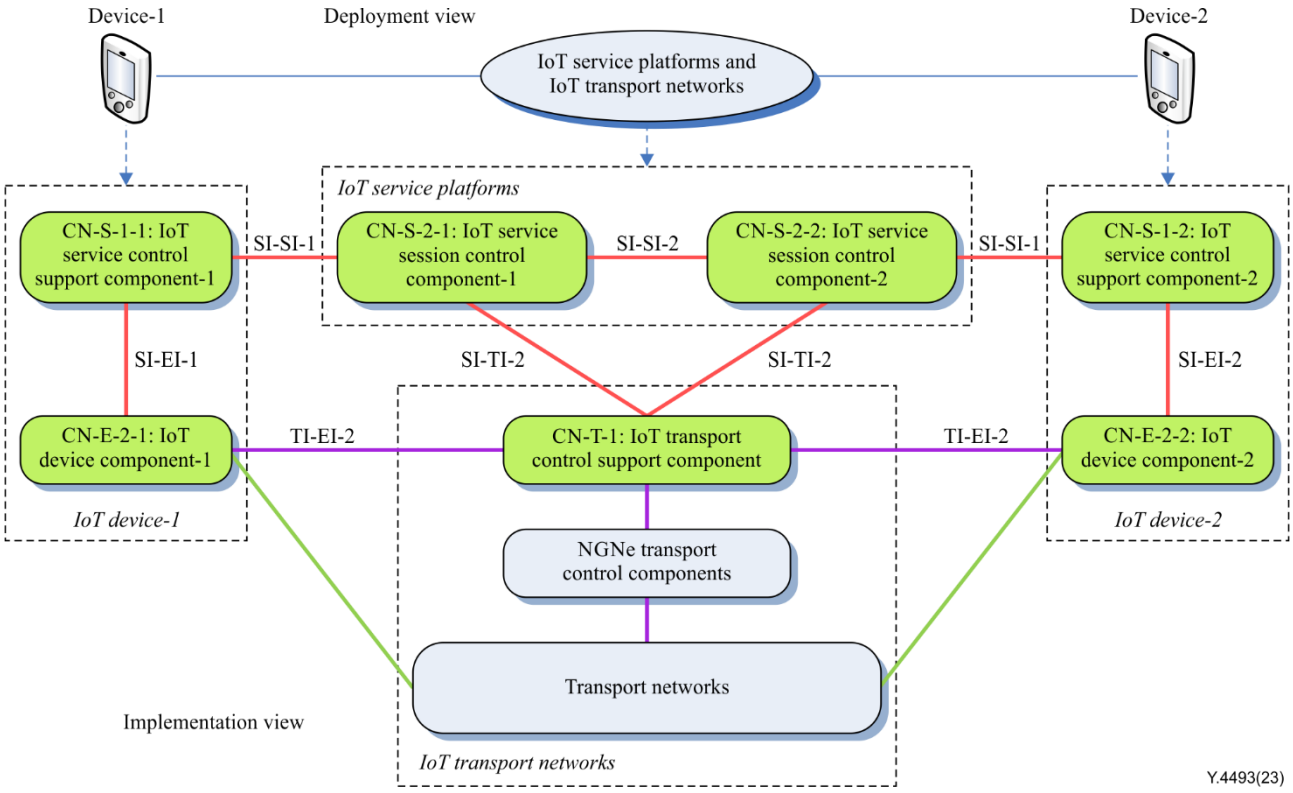

Figure I.1 – A use case of autonomic communication between IoT devices

The functional framework in the deployment view for autonomic communications in this use case consists of two IoT devices, and IoT service platforms and IoT transport networks as illustrated in Figure I.1.

The functional framework in the implementation view for autonomic communication in this use case consists of IoT device components and IoT service control support components implemented in IoT devices, IoT service session control components implemented in IoT service platforms, as well as the IoT transport control support component, next generation network evolution (NGNe) transport control components and transport networks implemented in the IoT transport networks, which are illustrated in Figure I.1. All of these IoT functional components are defined in clause 9 of [ITU-T Y.4416].

One possible message interaction of these IoT functional components to implement autonomic communication in this use case is shown in Figure I.2. The message interaction is described as follows.

(1) The CN-E-2-1 captures an event that makes a decision based on some related policies or knowledge to send a session initiation request to CN-S-1-1 deployed in IoT device-1 through the reference point SI-EI-1, by means of the AEM-SP specified in this Recommendation.

(2) The CN-S-1-1 forwards this request to the CN-S-2-1 deployed in the IoT service platforms through the reference point SI-SI-1 by means of the AC-SP specified in this Recommendation.

(3) This session request is validated in CN-S-2-1, and CN-S-2-1 sends a transport configuring request to CN-T-1 through the reference point SI-TI-2 by means of the AC-SP specified in this Recommendation.

(4) The CN-T-1 replies with the transport configuring response through the reference point SI-TI-2 to the CN-S-2-1 to inform that it cannot initiate session directly with IoT device-2.

(5) The CN-S-2-1 forwards the session request to the CN-S-2-2 through SI-SI-2 by means of the AC-SP specified in this Recommendation.

(6) This session request is validated by CN-S-2-2 and forwarded to CN-S-2-2, which sends a transport configuring request to the CN-T-1 through the reference point SI-TI-2 by means of the AC-SP specified in this Recommendation.

(7) The CN-T-1 replies with the transport configuring response through the reference point SI-TI-2 by means of the AC-SP specified in this Recommendation, so that the CN-S-2-2 can initiate session directly with IoT device-2.

(8) The CN-S-2-2 forwards this request to the CN-S-1-2 that is deployed in IoT device-2, through the reference point SI-SI-1 by means of the AC-SP specified in this Recommendation.

(9) This session request is validated by the CN-S-1-2 and delivered to the CN-E-2-2 deployed in IoT device-2 through the reference point SI-EI-2, by means of the AEM-SP specified in this Recommendation.

(10) The CN-E-2-2 validates the request to initiate a session from IoT device-1 to IoT device-2, and returns the session confirmed message to the CN-S-1-2 through the reference point SI-EI-2, by means of the AEM-SP specified in this Recommendation.

(11) This session initiation confirmed message is forwarded through CN-S-1-2, CN-S-2-2, CN-S-2-1 and CN-S-1-1 by means of the AC-SP specified in this Recommendation, and sent to the CN-E-2-1 deployed in IoT device-1 by means of the AEM-SP specified in this Recommendation.

(12) The transport connection request is sent from CN-E-2-1 through the reference point TI-EI-2 to CN-T-1, and forwarded through the reference point TI-EI-2 from CN-T-1 to CN-E-2-2 by means of the AC-SP specified in this Recommendation.

(13) The transport connection confirmed message is sent through the reference point TI-EI-2 from CN-E-2-2 to CN-T-1, and forwarded through the reference point TI-EI-2 from CN-T-1 to CN-E-2-1 by means of the AC-SP specified in this Recommendation.

(14) The IoT device-1 starts to communicate automatically with IoT device-2.

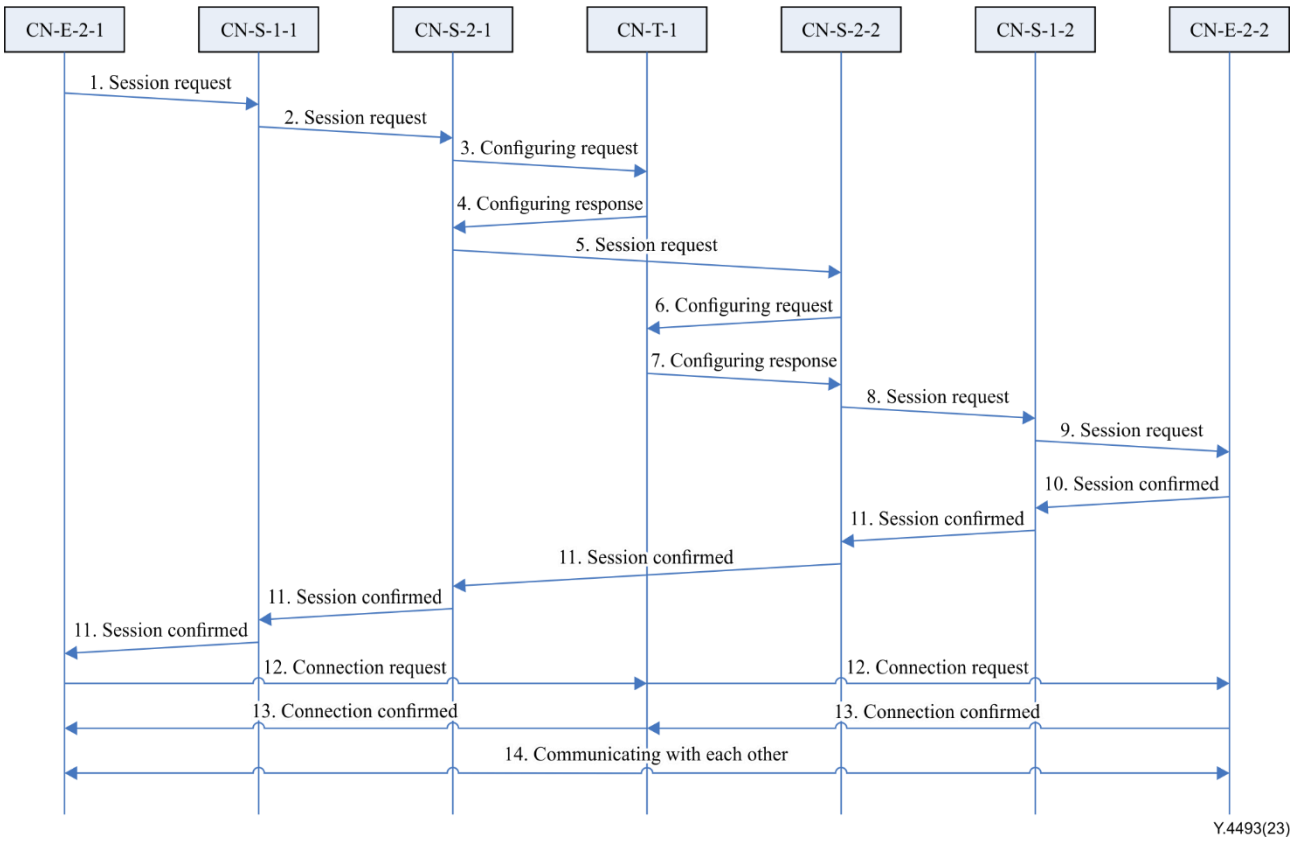

Figure I.2 – One scenario for autonomic communication

The preceding description of autonomic communication can be implemented by the AEM-SP and AC-SP specified in this Recommendation.

I.2 One possible deployment of autonomic operations support protocols

The message exchange described in the use case of the autonomic communication in clause I.1 can be implemented by the AEM-SP and AC-SP specified in this Recommendation as illustrated in Figure I.3.

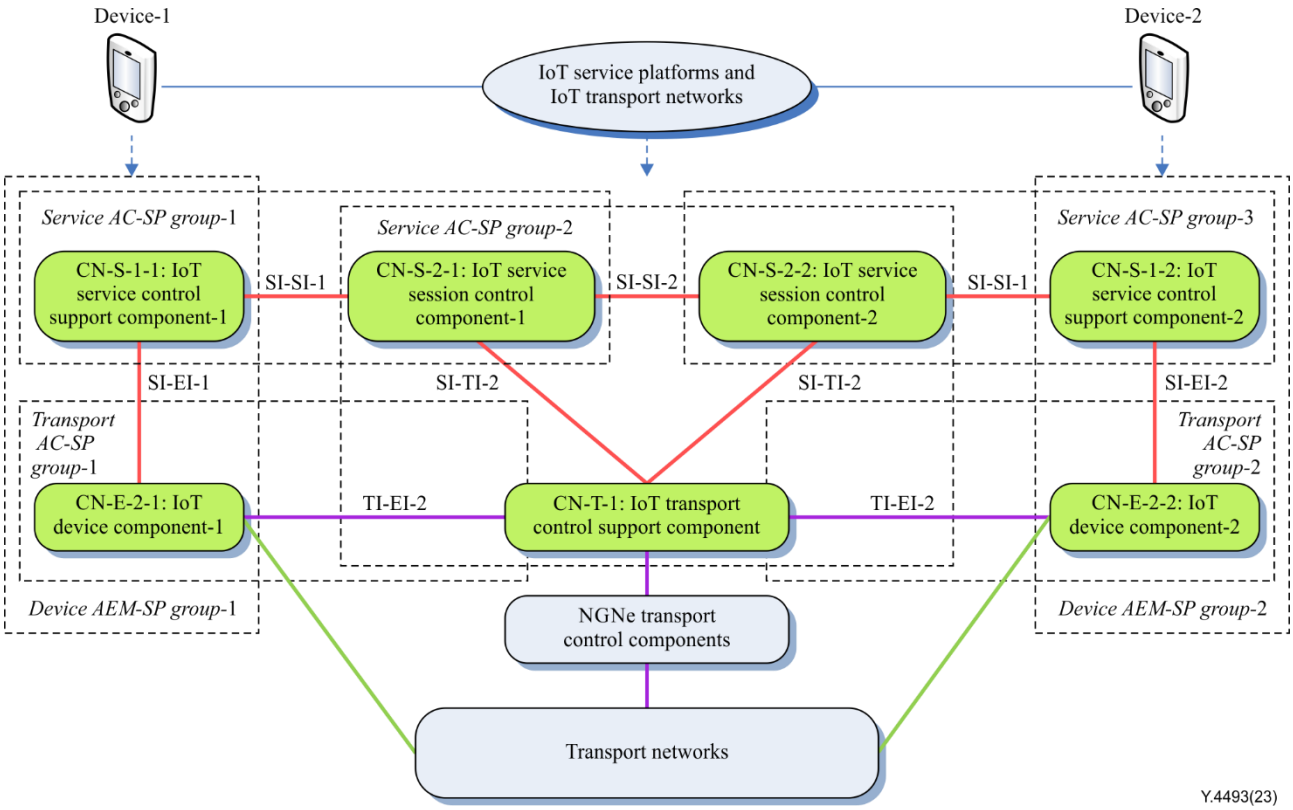

Figure I.3 – One possible deployment of autonomic control support protocol

From the IoT functional component perspective, the AC-SP is deployed in CN-S-1-1 and CN-S-1-2 of the IoT devices, in CN-S-2-1 and CN-S-2-2 of IoT service platforms, and in CN-T-1 of the IoT transport networks in this use case. The AEM-SP is deployed in CN-E-2-1 and CN-E-2-2 in the IoT devices, and in CN-S-1-1 and CN-S-1-2 of the IoT devices in this use case.

From the IoT operation perspective, the AEM-SP deployment in this use case includes device AEM-SP group-1 and device AEM-SP group-2. The device AEM-SP group-1 implements the reference point SI-EI-1 and the device AEM-SP group-2 implements the reference point SI-EI-2 as illustrated in Figure I.3.

From the IoT operation perspective, the AC-SP deployment in this use case includes transport AC-SP group-1, transport AC-SP group-2, service AC-SP group-1, service AC-SP group-2 and service AC-SP group-3. The two transport AC-SP groups implement the reference point TI-EI-2 as illustrated in Figure I.3. The service AC-SP group-1 and service AC-SP group-2 implement the reference point SI-SI-1 as illustrated in Figure I.3. The service AC-SP group-2 implements the reference point SI-TI-2 and SI-SI-2 as illustrated in Figure I.3.

Appendix II

Use cases of autonomic operations support protocols

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

Based on the use case of the IoT autonomic communication described in Appendix I, the use cases of the AEM-SP and the AC-SP are described in clauses II.1 and II.2, respectively.

II.1 A use case of AEM-SP

It is assumed that the AEM-SP has been deployed as described in Appendix I, and device AEM-SP group-1 and device AEM-SP group-2 has been established by using the functionalities of AEM-SP group management.

One possible message interaction of using the functionalities of AEM-SP event management to initiate a session in device-1 is shown in Figure II.1. The message interaction is described as follows.

1) The CN-E-2-1 in device-1 captures a timing event to send some data at a specified time to device-2, the CN-E-2-1 sends a session initiation request message to the device AEM-SP group-1. The CN-S-1-1 deployed in IoT device-1 receives the session initiation request message from the device AEM-SP group-1 and forwards it to the service AC-SP group-1.

2) The CN-S-1-1 in device-1 receives the session confirmed message from the service AC-SP group-1 and forwards it to the device AEM-SP group-1. The CN-E-2-1 in device-1 receives the session confirmed message from the device AEM-SP group-1.

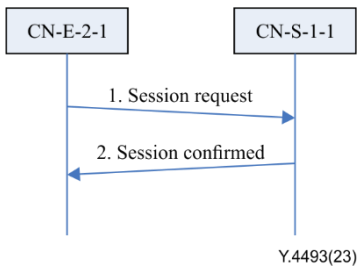

Figure II.1 – One scenario for initiating a session

II.2 A use case of AC-SP

It is assumed that the AC-SP has been deployed as described in Appendix I, and transport AC-SP group-1and transport AC-SP group-2 have been established by using the functionalities of AC-SP control management.

One possible message interaction of using the functionalities of AC-SP control management to establish a transport connection between device-1 and device-2 is shown in Figure II.2. The message interaction is described as follows.

1) The CN-E-2-1 in device-1 receives the session confirmed message from the device AEM-SP group-1 and sends a transport connection request to the transport AC-SP group-1. The CN-T-1 deployed in the IoT transport network receives the transport connection request from the transport AC-SP group-1 and forwards it to the transport AC-SP group-2.

2) The CN-E-2-2 in device-2 receives the transport connection request from the transport AC-SP group-2 and validates it.

3) The CN-E-2-2 in device-2 sends the transport connection confirmed message to transport AC-SP group-2. The CN-T-1 receives the transport connection confirmed message from the transport AC-SP group-2 and forwards it to the transport AC-SP group-1.

4) The CN-E-2-1 in device-1 receives the transport connection confirmed message from transport AC-SP group-1 and the transport connection between device-1 and device-2 is established.

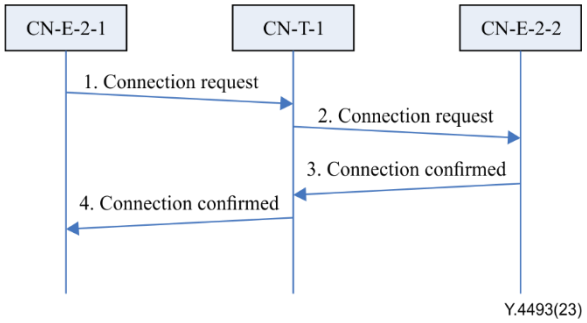

Figure II.2 – One scenario for establishing a transport connection

Bibliography

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024