INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION STANDARDIZATION SECTOR**

STUDY PERIOD 2022-2024

**SG20-TD935**

**STUDY GROUP 20**

**Original: English**

**Question(s):** 3/20 Arusha, 13-22 September 2023

**TD**

**Source:** Editors

**Title:** Output text of draft Recommendation ITU-T Y.IoT-AOS-prot "Autonomic operations support protocols in the Internet of things", Q3/20 meeting (Arusha, 13-22 September 2023) - for consent

**Contact:** Subin SHEN
NUPT
China
Tel: +86-25-83492137
E-mail: sbshen@njupt.edu.cn

**Contact:** Xueqin JIA
China Unicom
China
Tel: +86-10-68799999
Email: jiaxq21@chinaunicom.cn

**Contact:** Younghwan Choi
ETRI
Korea (Republic of)
Tel: +82-42-860-1429
Fax: +82-42-861-5404
Email: yhc@etri.re.kr

**Abstract:** This TD contains the output text of draft Recommendation ITU-T Y.IoT-AOS-prot "Autonomic operations support protocols in the Internet of things", Q3/20 meeting (Arusha, 13-22 September 2023) - for consent. This text is based on the output text of draft Recommendation ITU-T Y.IoT-AOS-prot, SG20-TD580/GEN and Contribution C298R1.

The following table reflects discussion results based on the contribution.

| Contribution. No. | Contribution title and proposals | Agreements & Comments |
|---|---|---|
| C298R1 | Proposal for the consent version of draft Recommendation ITU-T Y.IoT-AOS-prot "Autonomic operations support protocols in the Internet of things"<br>- Completion of Appendix I<br>- Completion of Appendix II | − Agreed. |

The following table shows discussion results from the floor.

| No. | Comment | Agreements |
|---|---|---|
| 1 | - The connection between the protocols specified in this draft Recommendation and the IoT protocols that have been | - The protocols specified in this draft Recommendation are based on the IoT architecture specified in Y.4416. There is no connection with other IoT |

| | | |
|---|---|---|
| | standardized, such as M2M protocols, should be clarified. | protocols that have been standardized. |

# Draft Recommendation ITU-T Y.IoT-AOS-prot

## Autonomic operations support protocols in the Internet of things

**Summary**

This draft Recommendation provides a description of the 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. It describes architecture of autonomic operations support protocols in the IoT, autonomic event management support protocol, autonomic control support protocol, and autonomic policy management support protocol in the IoT. Possible deployment and relevant use cases of these autonomic operations support protocols in the IoT are described.

**Keywords**

Autonomic operation; event management; Internet of things; policy management; protocols

**CONTENTS**

**Page**

# Draft Recommendation ITU-T Y.IoT-AOS-prot

## Autonomic operations support protocols in the Internet of things

### 1 Scope

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

The scope of this draft 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;

Security of autonomic operations support protocols in 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; all 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.

[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 document uses the following terms 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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

### 3.2 Terms defined in this Recommendation

This document defines the following terms:

None

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| AC-SP | Autonomic Control Support Protocol |
| AEM-SP | Autonomic Event Management Support Protocol |
| APM-SP | Autonomic Policy Management Support Protocol |
| IoT | Internet of things |
| NGN | Next Generation Network |

## 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 functional entities of the IoT architecture specified in [ITU-T Y.4416], the relations of these functional entities 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 with 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. The autonomic operations support protocols can be classified into autonomic event management support protocol (AEM-SP), autonomic control support protocol (AC-SP), and autonomic policy management support protocol (APM-SP).

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

TI-1, and SI-DI-1.

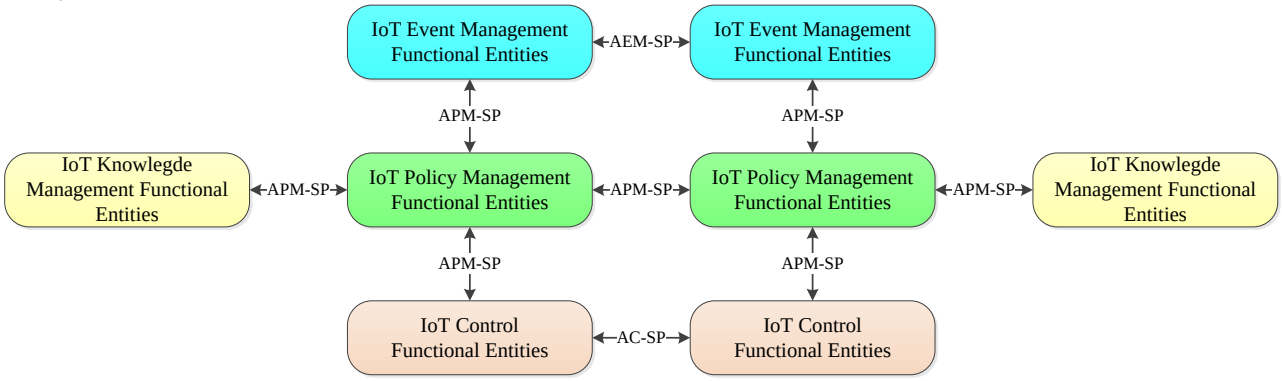


**Figure 6-1 Architecture of autonomic operations support protocols**

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

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

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

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

The APM-SP can also be used among distributed implementations of the same type of IoT policy management functional entities 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 these reference points that are among or between IoT functional entities extended to support IoT capabilities in [ITU-T Y.4416]. These three protocols do not implement all reference point related to the functional entities of next generation network (NGN) evolution that are enhanced to support IoT capabilities in [ITU-T Y.4416]. So specifications of the all protocols that are based on NGN evolution are out of the scope of this Recommendation.

### 6.2 Functions of autonomic event management support protocol

Autonomic event management support protocol (AEM-SP) can be used to implement reference points among IoT event management functional entities, which include IoT end-point event management functional entity (IoT-EEM-FE), IoT transport event management functional entity (IoT-TEM-FE), IoT data event management functional entity (IoT-DEM-FE), and IoT service event management

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

The functions of AEM-SP include:

– Collecting events occurred in different IoT functional layers in order to support cross-layer IoT event capturing.

– Collecting events occurred in distributed implementations of the same type of IoT event management functional entities in order to support distributed IoT event capturing.

– Collaborating events processing with other event management functional entities 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 functional entities in order to support distributed IoT event processing.

### 6.3 Functions of autonomic control support protocol

Autonomic control support protocol (AC-SP) can be used to implement the reference points among IoT control functional entities, which include IoT end-point access control functional entity (IoT-EAC-FE), IoT transport configuration adaptation functional entity (IoT-TCA-FE), IoT data service adaptation functional entity (IoT-DSA-FE), and IoT service provision adaptation functional entity (IoT-SPA-FE). All these IoT control-related functional entities 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 functional entities 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 functional entities 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

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

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

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

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

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

The functions of APM-SP include:

– Controlling and obtaining new knowledge learned in the IoT knowledge management functional entities 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 functional entities in order to support distributed policy enforcement on the IoT autonomic operations.

– Collaborating with IoT event management functional entities in order to support the functions of IoT autonomic operations with help of policy-enforced IoT event management capabilities.

– Collaborating with IoT control functional entities in order to support the functions of IoT autonomic operations with 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 is out of scope of this Recommendation.

# 7 Autonomic event management support protocol

## 7.1 Scope of autonomic event management support protocol

The scope of autonomic event management support protocol (AEM-SP) includes following two aspects.

– Exchange event management messages among IoT event management functional entities 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 event management message among the IoT event management functional entities 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.

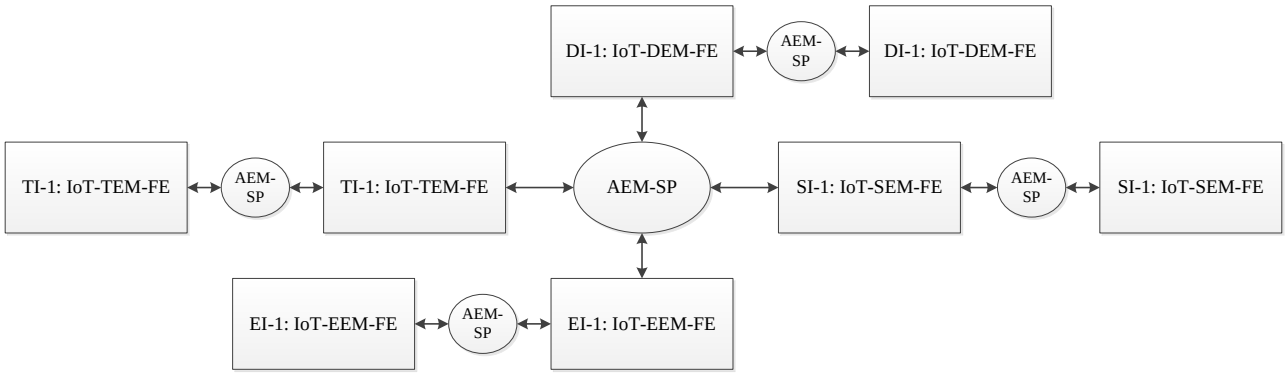


**Figure 7-1 Scope of autonomic event management support protocol (AEM-SP)**

The scope of AEM-SP is illustrated in figure 7-1. The IoT event management functional entities illustrated in this figure, 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].

## 7.2 The features of autonomic event management support protocol

The autonomic event management support protocol (AEM-SP) includes following features.

– The AEM-SP is a group protocol (as illustrated in figure 7-1) that can send messages to several IoT event management functional entities that belong to one group.

– Different AEM-SP group can be established to manage different types of events.

## 7.3 The message structure of autonomic event management support protocol

The message structure of autonomic event management support protocol (AEM-SP) consists of message head and message body. The message head consists of AEM-SP identifier (AEM-SP-ID, 8bits), 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 AEM-SP is illustrated in figure 7-2.

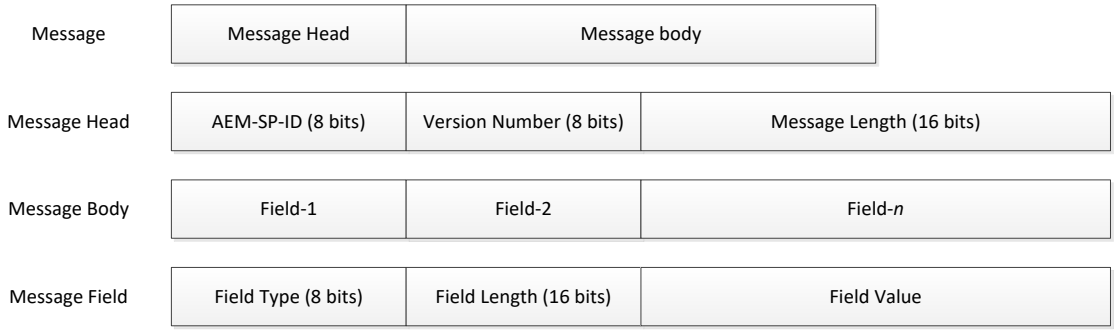


**Figure 7-2 message structure of AEM-SP**

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

### 7.3.1 The basic fields of AEM-SP group management category

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

NOTE 1 – The “group address” can be any type of existing group address or self-defined group address either in network functional layer or in application functional layer.

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 will not specify the field type in detail.

### 7.3.2 The basic fields of event management category

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

### 7.4 The functionalities of autonomic event management support protocol

The functionalities of autonomic event management support protocol (AEM-SP) can be classified into the AEM-SP group management functionalities and the AEM-SP event management functionalities, based on the scope and feature of AEM-SP.

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

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

#### 7.4.1 The functionalities of AEM-SP group management

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

(1) Assigning group managers

The group managers refer to the entities of AEM-SP that can establish and update the group of AEM-SP, and store and update the information of the group. The group managers include one active group manager and several backup group managers.

Assigning group managers is to initiate an active group manager and assign at least one backup manager for the group during the initiation stage of AEM-SP. The group managers should perform the following operations:

- The active group manager should broadcast announcement message to announce the group address periodically.
- The active group manager should listen to new-member message on the group address and prepare to adopt new group members to join in this group.
- The active group manager should be able to authenticate the new group members when it is required based on the requirements of some special security level.
- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The backup group managers should listen to the messages sent by the active group managers and prepare to take the role of an active group manager when the current active group manager have not been in active.

(2) Updating group manager

Updating group manager is to update configuration of the active group manager or the backup group managers, and to replace the active group manager with one backup group manager. Updating the configuration of the active group manager or the 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 one of the functionalities of AEM-SP, which should perform following operations.

- The backup group managers should listen to both announcement messages and heartbeat messages sent by the active group managers.
- The backup group managers should compete for new active group manager when neither announcement messages nor heartbeat messages have been received for a period of time.
- The competent backup group manager should take the role of the active group manager and perform all the operations that the active group manager should do.

(3) Adding group members

Adding group members is to listen to new-member message on the group address, authenticate the new group member when it is necessary, and update the group information when the 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 message broadcasted by the active group manager.
- The new AEM-SP entity should send the new-member message on the group address.
- The new AEM-SP entity should provide the authentic data that can be authenticated by the active group manager when it is required based on the requirements of some special security level.

(4) Updating group members

Updating group members is to check the active status of all group members, delete inactive group members, and update the group information when the inactive group members have been deleted. In order to provide the functionality of updating group members, the following operations should be supported.

- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The group members should receive the heartbeat messages in time.
- The group members should reply to the received heartbeat messages in time.

(5) Multicasting message within the group

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

- The active group manager should receive event management messages on all group addresses belong to this group.
- The active group manager should transfer the event management messages to all group addresses within the group except for the group address from that the event management messages have been received.

### 7.4.2 The functionalities of AEM-SP event management

The functionalities of AEM-SP event management include the functionalities 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 is to prepare an event messages and send the message to the 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 the event information and encode it into event messages.
- The AEM-SP entity should identify the types of events and select the group for sending event messages to it based on predefined event management policies and the knowledge learned by machine on event management.
- The AEM-SP entity should send the event messages on the addresses of selected groups.

(2) Receiving event messages

Receiving event messages is to identify the events in the event messages and deliver them to the corresponding event management entities. Receiving event messages is also to identify the groups bound by the event type in the event messages and determine whether it is necessary to transfer this event message to other groups that are different from the group receiving the event messages, when the AEM-SP entity receiving the event messages play a role of 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 received event messages and deliver them to the corresponding event management entities based on predefined event management policies and the knowledge learned by machine on event management.
- The active group managers identify the groups bound by the event type in this event messages and make a decision on whether it is necessary to transfer the event messages to other groups that are different from the group receiving the event messages.

(3) Transferring event messages

Transferring event messages is to check the relevant groups in which there is no event message that is similar to the received event messages and transfer 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 received event messages.
- 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 find out all groups in which there is no event message that is similar to the received event messages.
- 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 is to bind the 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 a type or several types of events to some event management groups should encode all necessary data related to binding the events to groups into a group binding message.
- The AEM-SP entity that needs to bind a type or more types of events to some event management groups should send the group binding message to the groups bound by the event or events in the group binding message.
- The active group manager that has received a group binding message should initiate an event type and event group management table if there is no such table 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 event type and event group management table if the table had been established, by adding all the binding relations in the group binding message to the table.

(5) Unbinding events from groups

Unbinding events to groups is to unbind the event types from the event management groups in 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 a type or several types of events from some event management groups should encode all necessary data related to unbinding the events from groups into a group unbinding message.
- The AEM-SP entity that needs to unbind a type or more types of events from some event management groups should send the group unbinding message to the groups unbound from the event or events in the group unbinding message.
- The active group manager that has received a group unbinding message should update the event type and event group management table if there is no such table, by deleting 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 autonomic control support protocol (AC-SP) includes following two aspects.

– Exchange control messages among IoT control functional entities 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 control message among IoT control functional entities 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.

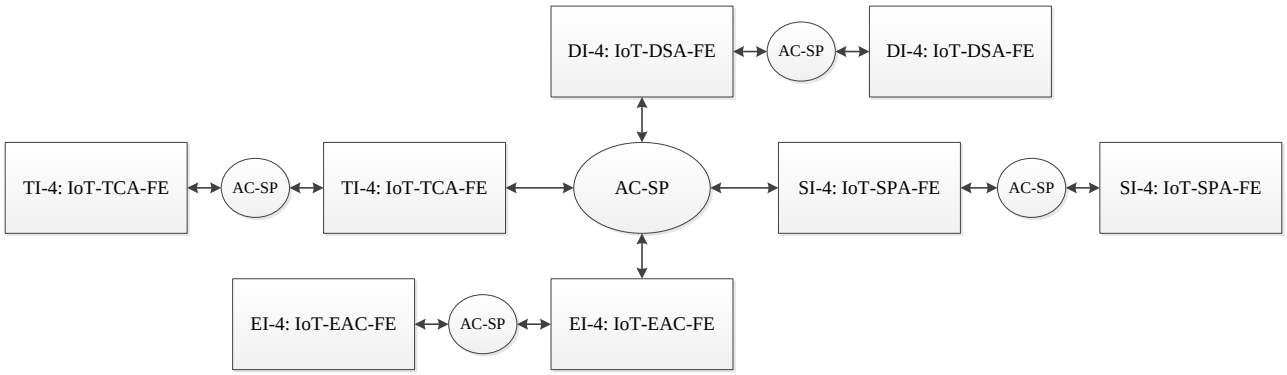


**Figure 8-1 Scope of autonomic control support protocol (AC-SP)**

The scope of AC-SP is illustrated in figure 8-1. The IoT control functional entities illustrated in this figure, 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].

## 8.2 The features of autonomic control support protocol

The autonomic control support protocol (AC-SP) includes following features.

– The AC-SP is a group protocol (as illustrated in figure 8-1) that can send messages to several IoT control functional entities that belong to one group.

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

## 8.3 The message structure of autonomic control support protocol

The message structure of autonomic control support protocol (AC-SP) consists of message head and message body. The message head consists of AC-SP identifier (AC-SP-ID, 8bits), 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.

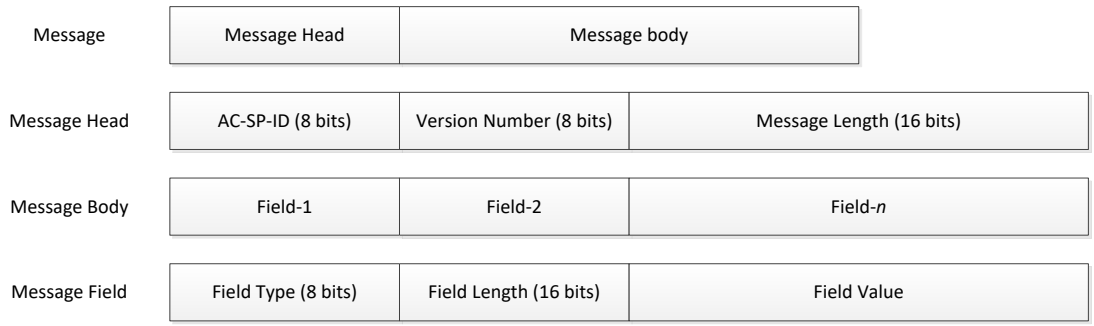


**Figure 8-2 message structure of AC-SP**

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

### 8.3.1 The basic fields of AC-SP group management category

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

NOTE 1 – The "group address" can be any type of existing group address or self-defined group address either in network functional layer or in application functional layer.

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 will not specify the field type in detail.

### 8.3.2 The basic fields of single-layer control coordination category

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

NOTE 1 – The "control data" includes the text describing the purposes and features of the control, and the rules enforced by the control.

### 8.3.3 The basic fields of cross-layer control coordination category

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

NOTE 1 – The "control data" includes the text describing the purposes and features of the control, and the rules enforced by the control.

## 8.4 The functionalities of autonomic control support protocol

The functionalities of autonomic control support protocol (AC-SP) can be classified into the AC-SP group management functionalities and the AC-SP control coordination functionalities, based on the scope and feature of AC-SP.

NOTE 1 – The AC-SP is specified as a self-containment protocol. The specifications of the AC-SP do not depend on any existing protocol. The implementation of the AC-SP can rely on the implementation of an existing protocols to multicast the AC-SP messages within the control group. The mechanisms or methods of implementing the AC-SP are out of the scope of this draft Recommendation.

### 8.4.1 The functionalities of AC-SP group management

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

(1) Assigning group managers

The group managers are defined as the entities of AC-SP that can establish and update the group of AC-SP, and store and update the information of the group. The group managers include one active group manager and several backup group managers.

Assigning group managers is to initiate an active group manager and assign at least one backup manager for the group during the initiation stage of AC-SP. The group managers should perform the following operations:

- The active group manager should broadcast announcement message to announce the group address periodically.
- The active group manager should listen to new-member message on the group address and prepare to adopt new group members to join in this group.
- The active group manager should be able to authenticate the new group members when it is required based on the requirements of some special security level.
- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The backup group managers should listen to the messages sent by the active group managers and prepare to take the role of an active group manager when the current active group manager have not been in active.

(2) Updating group manager

Updating group manager is to update configuration of the active group manager or the backup group managers, and to replace the active group manager with one backup group manager. Updating the configuration of the active group manager or the 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 one of the functionalities of AC-SP, which should perform following operations.

- The backup group managers should listen to both announcement messages and heartbeat messages sent by the active group managers.
- The backup group managers should compete for new active group manager when neither announcement messages nor heartbeat messages have been received for a period of time.
- The competent backup group manager should take the role of the active group manager and perform all the operations that the active group manager should do.

(3) Adding group members

Adding group members is to listen to new-member message on the group address, authenticate the new group member when it is necessary, and update the group information when the 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 message broadcasted by the active group manager.
- The new AC-SP entity should send the new-member message on the group address.
- The new AC-SP entity should provide the authentic data that can be authenticated by the active group manager when it is required based on the requirements of some special security level.

(4) Updating group members

Updating group members is to check the active status of all group members, delete inactive group members, and update the group information when the inactive group members have been deleted. In order to provide the functionality of updating group members, the following operations should be supported.

- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The group members should receive the heartbeat messages in time.
- The group members should reply to the received heartbeat messages in time.

(5) Multicasting message within the group

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

- The active group manager should receive control coordination messages on all group addresses belong to this group.
- The active group manager should transfer the control coordination messages to all group addresses within the group except for the group address from that the control coordination messages have been received.

### 8.4.2 The functionalities of AC-SP control coordination

The functionalities of AC-SP control coordination include the functionalities 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 is to prepare an control coordination messages and send the message to the 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 the control information and encode it into control coordination messages.
- The AC-SP entity should identify the types of controls and select the group for sending control coordination messages to it based on predefined control coordination policies and the knowledge learned by machine on control coordination.
- The AC-SP entity should send the control coordination messages on the addresses of selected groups.

(2) Receiving control coordination messages

Receiving control coordination messages is to identify the controls in the control coordination messages and deliver them to the corresponding control related entities. Receiving control coordination messages is also to identify the groups bound by the control type in the control coordination messages and determine whether it is necessary to transfer this control coordination message to other groups that are different from the group receiving the control coordination messages, when the AC-SP entity receiving the control coordination messages play a role of 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 received control coordination messages and deliver them to the corresponding control related entities based on predefined control coordination policies and the knowledge learned by machine on control coordination.
- The active group managers identify the groups bound by the control type in this control coordination messages and make a decision on whether it is necessary to transfer the control coordination messages to other groups that are different from the group receiving the control coordination messages.

(3) Transferring control coordination messages

Transferring control coordination messages is to check the relevant groups in which there is no control coordination message that is similar to the received control coordination messages and transfer 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 received control coordination messages.
- 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 find out all groups in which there is no control coordination message that is similar to the received control coordination messages.
- The active group manager that has received control coordination messages should transfer the control coordination messages 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 is to bind the control types to the control coordination groups in 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 a type or several types of controls to some control coordination groups should encode all necessary data related to binding the controls to groups into a group binding message.
- The AC-SP entity that needs to bind a type or more types of controls to some control coordination groups should send the group binding message to the groups bound by the control or controls in the group binding message.
- The active group manager that has received a group binding message should initiate an control type and control coordination group management table if there is no such table 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 the table had been established, by adding all the binding relations in the group binding message to the table.

(5) Unbinding controls from groups

Unbinding controls to groups is to unbind the control types from the control coordination groups in 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 a type or several types of controls from some control coordination groups should encode all necessary data related to unbinding the controls from groups into a group unbinding message.
- The AC-SP entity that needs to unbind a type or more types of controls from some control coordination groups should send the group unbinding message to the groups unbound from the control or controls in the group unbinding message.
- The active group manager that has received a group unbinding message should update the control type and control coordination group management table if there is no such table, by deleting all the binding relations in the group binding message from the table.

# 9 Autonomic policy management support protocol

## 9.1 Scope of autonomic policy management support protocol

The autonomic policy management support protocol (APM-SP) is in the center of autonomic operations support protocol as illustrated in figure 6-1. The scope of APM-SP can be classified into two parts: implementation of reference points among the policy enforcement functional entities that are specified in [ITU-T Y.4416], and implementation of reference points between the policy enforcement functional entities and other functional entities that are specified in [ITU-T Y.4416]. The scope of the first part of APM-SP includes following two aspects.

– Exchange policy enforcement messages among IoT policy enforcement functional entities 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 policy enforcement message among IoT policy enforcement functional entities 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.

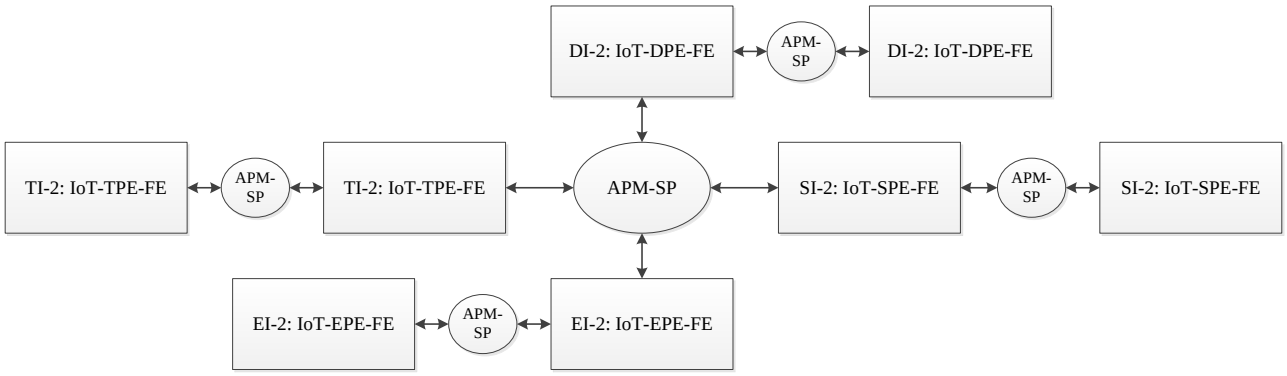


**Figure 9-1 Scope of autonomic policy management support protocol (APM-SP) – part I**

The scope of the first part of APM-SP is illustrated in figure 9-1. The IoT policy enforcement functional entities illustrated in this figure, 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].

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

– Exchange policy enforcement messages between IoT policy enforcement functional entities and IoT knowledge management functional entities within the same functional layer, in order to coordinate policy enforcement operations on the IoT knowledge management in the same functional layer and update IoT policies in the IoT policy enforcement functional entities.

– Exchange policy enforcement messages between IoT policy enforcement functional entities and IoT event management functional entities within the same functional layer, in order to coordinate policy enforcement operations on the 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 functional entities and IoT control functional entities within the same functional layer, in order to coordinate policy enforcement operations on the IoT control in the same functional layer, and make decision on initiating and controlling autonomic operations.

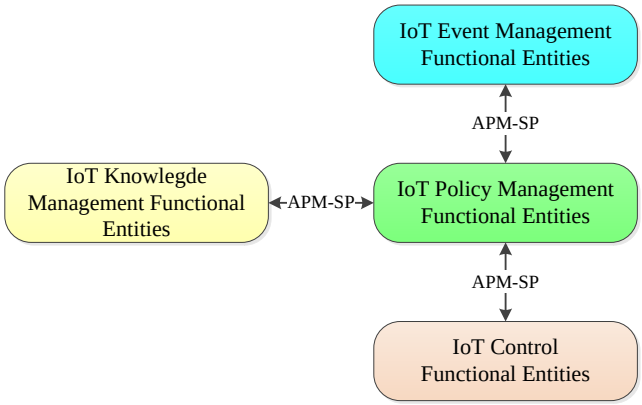


**Figure 9-2 Scope of autonomic policy management support protocol (APM-SP) – part II**

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

### 9.2 The features of autonomic policy management support protocol

The autonomic policy management support protocol (APM-SP) includes following features.

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

– Different APM-SP group 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 functional entities, as illustrated in figure 9-2.

### 9.3 The message structure of autonomic policy management support protocol

The message structure of autonomic policy management support protocol (APM-SP) consists of message head and message body. The message head consists of APM-SP identifier (APM-SP-ID, 8bits), 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 APM-SP is illustrated in figure 9-3.

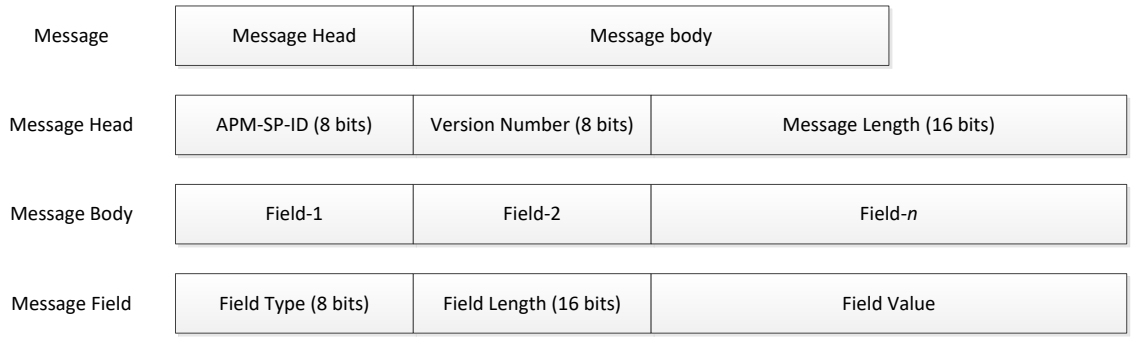


**Figure 9-3 message structure of APM-SP**

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

### 9.3.1 The basic fields of APM-SP group management category

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

NOTE 1 – The "group address" can be any type of existing group address or self-defined group address either in network functional layer or in application functional layer.

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 will not specify the field type in detail.

### 9.3.2 The basic fields of policy management category

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

### 9.3.3 The basic fields of policy-enforced knowledge learning category

The basic fields of 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 The basic fields of policy-enforced event management category

The basic fields of 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 The basic fields of policy-enforced control category

The basic fields of 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 The functionalities of autonomic policy management support protocol

The functionalities of autonomic policy management support protocol (APM-SP) can be classified into the APM-SP group management functionalities and the APM-SP policy enforcement functionalities, based on the scope and feature of APM-SP.

NOTE 1 – The functionalities of APM-SP specified in this clause are related to the message exchange among the IoT policy enforcement functional entities, which are different from the IoT policy enforcement functions specified in the IoT policy enforcement functional entities. The IoT policy enforcement functional entities had been specified in [ITU-T Y.4416].

### 9.4.1 The functionalities of APM-SP group management

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

(1) Assigning group managers

The group managers refer to the entities of APM-SP that can establish and update the group of APM-SP, and store and update the information of the group. The group managers include one active group manager and several backup group managers.

Assigning group managers is to initiate an active group manager and assign at least one backup manager for the group during the initiation stage of APM-SP. The group managers should perform the following operations:

- The active group manager should broadcast announcement message to announce the group address periodically.
- The active group manager should listen to new-member message on the group address and prepare to adopt new group members to join in this group.
- The active group manager should be able to authenticate the new group members when it is required based on the requirements of some special security level.
- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The backup group managers should listen to the messages sent by the active group managers and prepare to take the role of an active group manager when the current active group manager have not been in active.

(2) Updating group manager

Updating group manager is to update configuration of the active group manager or the backup group managers, and to replace the active group manager with one backup group manager. Updating the configuration of the active group manager or the 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 one of the functionalities of APM-SP, which should perform following operations.

- The backup group managers should listen to both announcement messages and heartbeat messages sent by the active group managers.
- The backup group managers should compete for new active group manager when neither announcement messages nor heartbeat messages have been received for a period of time.

- The competent backup group manager should take the role of the active group manager and perform all the operations that the active group manager should do.

(3) Adding group members

Adding group members is to listen to new-member message on the group address, authenticate the new group member when it is necessary, and update the group information when the 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 message broadcasted by the active group manager.
- The new APM-SP entity should send the new-member message on the group address.
- The new APM-SP entity should provide the authentic data that can be authenticated by the active group manager when it is required based on the requirements of some special security level.

(4) Updating group members

Updating group members is to check the active status of all group members, delete inactive group members, and update the group information when the inactive group members have been deleted. In order to provide the functionality of updating group members, the following operations should be supported.

- The active group manager should send heartbeat messages periodically to all the group members for checking whether they are active.
- The group members should receive the heartbeat messages in time.
- The group members should reply to the received heartbeat messages in time.

(5) Multicasting message within the group

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

- The active group manager should receive policy enforcement messages on all group addresses belong to this group.
- The active group manager should transfer the policy enforcement messages to all group addresses within the group except for the group address from that the policy enforcement messages have been received.

### 9.4.2 The functionalities of APM-SP policy enforcement

The functionalities of APM-SP policy enforcement include the functionalities 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 is to prepare a policy enforcement message and send the message to the 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 the policy enforcement information and encode it into policy enforcement messages.
- The APM-SP entity should identify the types of policy enforcements and select the group for sending policy enforcement messages to it based on human-defined policies.
- The APM-SP entity should send the policy enforcement messages on the addresses of selected groups.

(2) Receiving policy enforcement messages

Receiving policy enforcement messages is to identify the policy enforcements in the policy enforcement messages and deliver them to the corresponding policy enforcement entities. Receiving policy enforcement messages is also to identify the groups bound by the policy enforcement type in the policy enforcement messages and determine whether it is necessary to transfer this policy enforcement message to other groups that are different from the group receiving the policy enforcement messages, when the APM-SP entity receiving the policy enforcement messages play a role of 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 received policy enforcement messages and deliver them to the corresponding policy enforcement entities based on human-defined policies.
- The active group managers identify the groups bound by the policy enforcement type in this policy enforcement messages and make a decision on whether it is necessary to transfer the policy enforcement messages to other groups that are different from the group receiving the policy enforcement messages.

(3) Transferring policy enforcement messages

Transferring policy enforcement messages is to check the relevant groups in which there is no policy enforcement message that is similar to the received policy enforcement messages and transfer 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 received policy enforcement messages.
- 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 find out all groups in which there is no policy enforcement message that is similar to the received policy enforcement messages.
- 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 is to bind the 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 a type or several types of policy enforcements to some policy enforcement groups should encode all necessary data related to binding the policy enforcements to groups into a group binding message.
- The APM-SP entity that needs to bind a type or more types of policy enforcements to some policy enforcement groups should send the group binding message to the groups bound by the policy enforcement or policy enforcements in the group binding message.
- The active group manager that has received a group binding message should initiate a policy enforcement type and policy enforcement group management table if there is no such table 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 the table had been established, by adding all the binding relations in the group binding message to the table.

(5) Unbinding policy enforcements from groups

Unbinding policy enforcements to groups is to unbind the policy enforcement types from the policy enforcement groups in 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 a type or several types of policy enforcements from some policy enforcement groups should encode all necessary data related to unbinding the policy enforcements from groups into a group unbinding message.
- The APM-SP entity that needs to unbind a type or more types of policy enforcements from some policy enforcement groups should send the group unbinding message to the groups unbound from the policy enforcement or policy enforcements in the group unbinding message.
- The active group manager that has received a group unbinding message should update the policy enforcement type and policy enforcement group management table if there is no such table, by deleting all the binding relations in the group binding message from the table.

## 10 Security consideration

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

(1) The definition of group security level. The “group security level” has been defined in the message structure of the autonomic event management support protocol (AEM-SP), the message structure of the autonomic control support protocol (AC-SP), and the message structure of the autonomic policy management support protocol (APM-SP). The “group security level” can be used to introduce possible security related capabilities into the autonomic operation support protocols in order to satisfy the security requirements from some specific applications.

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

(3) The specification of message structure of cross-layer control coordination. In the message structure of autonomic control support protocol (AC-SP), the basic fields of cross-layer control coordination category have been specified to include control coordinator identifier, coordinator-layer identifier, relevant control entity identifier, relevant control layer identifier, control classifier (such as end-point, transport, data, service, etc.), relevant-event identifier, 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

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

The 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 the possible deployment of the 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 initiate automatically 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.

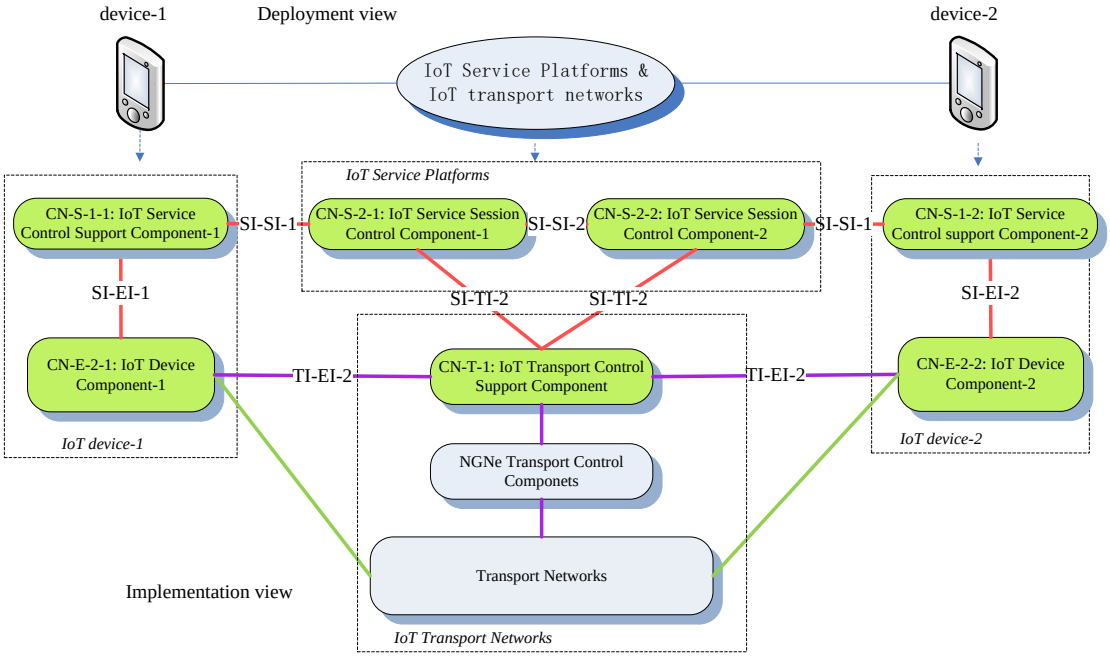


**Figure I.1 – A use case of autonomic communication between IoT devices**

The functional framework in the deployment view for the 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 the autonomic communication in this use case consists of the IoT device components and the IoT service control support components implemented in the IoT devices, the IoT service session control components implemented in the IoT service platforms, and the IoT transport control support component, NGNe transport control components, and transport networks implemented in the IoT transport networks, which are illustrated in Figure I.1. All 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 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 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 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 AC-SP specified in this Recommendation.

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

(10) The CN-E-2-2 validates the request for initiating 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 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 AC-SP specified in this Recommendation, and sent to the CN-E-2-1 deployed in IoT device-1 by means of 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 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 AC-SP specified in this Recommendation.

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

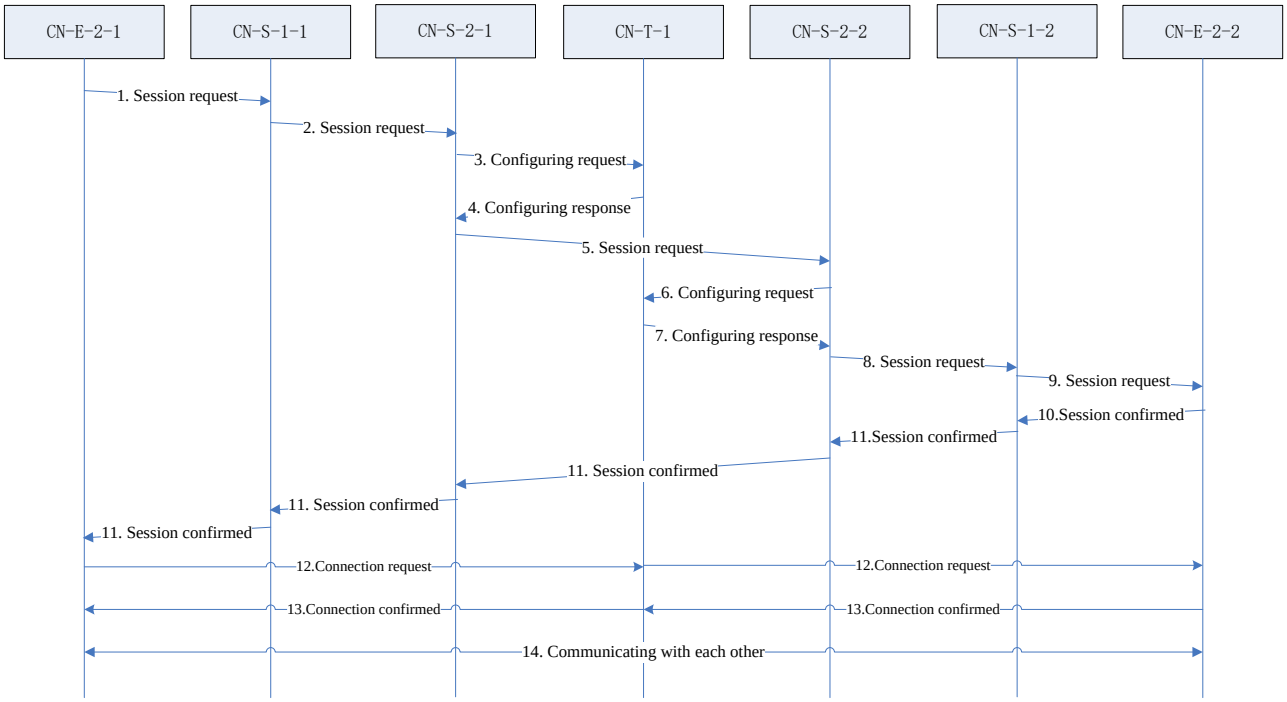


Figure I.2 – One scenario for autonomic communication

The above description of the autonomic communication can be implemented by 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 I.1 can be implemented by AEM-SP and AC-SP specified in this Recommendation as illustrated in Figure I.3.

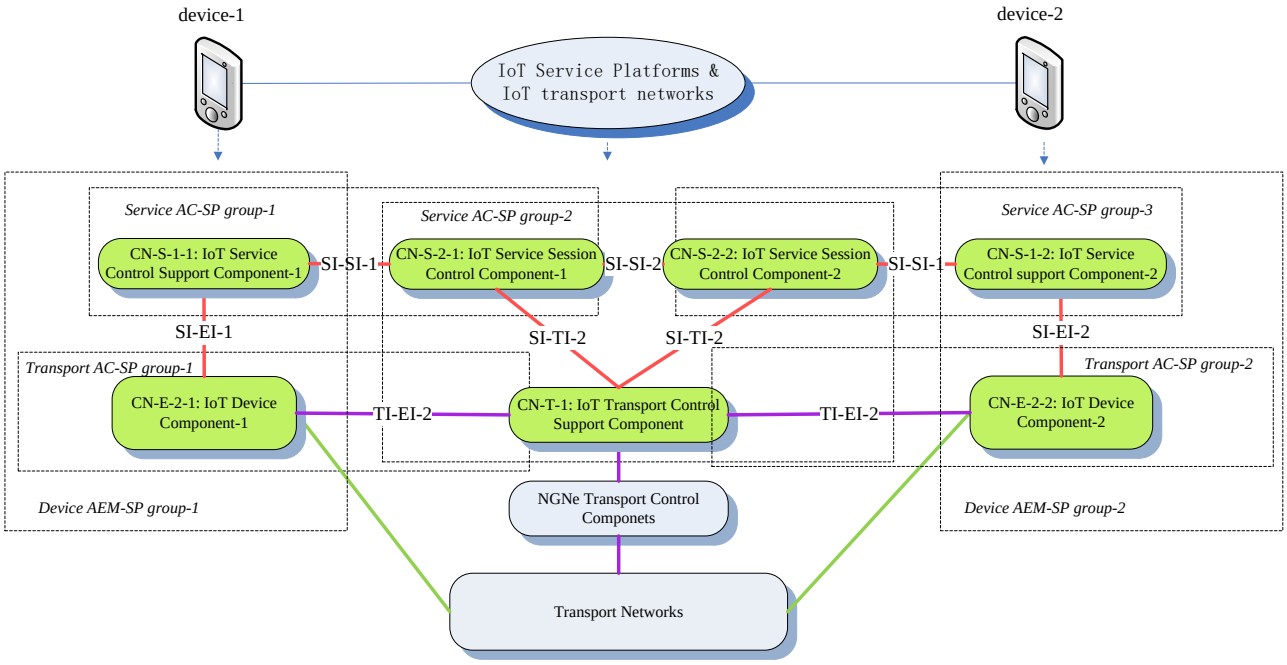

Figure I.3 One possible deployment of autonomic control support protocol

In 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.

In 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.

In 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

(Note: 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 of this Recommendation, the use cases of autonomic event management support protocol (AEM-SP) and autonomic control support protocol (AC-SP) are described as follows.

### II.1 A use case of AEM-SP

It is assumed that the AEM-SP has been deployed as described in Appendix I of this Recommendation, 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 the 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 forward 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 forward 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.

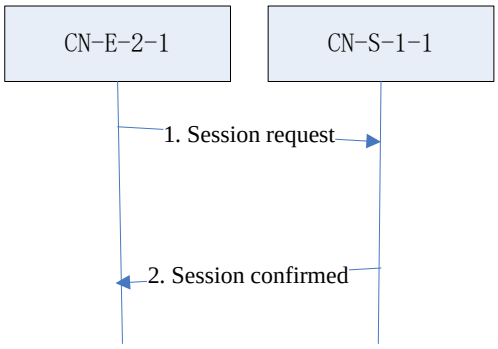


**Figure II.1 – One scenario for initiating a session**

### II.2 A use case of AC-SP

It is assumed that the AC-SP has been deployed as described in Appendix I of this Recommendation, and transport AC-SP group-1and transport AC-SP group-2 has 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 forwarded 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 the transport connection request.

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

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

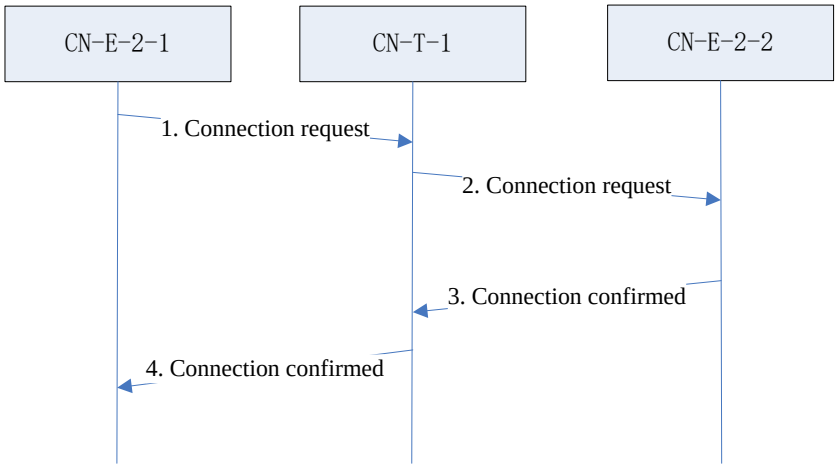


**Figure II.2 – One scenario for establishing a transport connection**

## Bibliography

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

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

_____