International Telecommunication Union

ITU-T
Q.3711
(08/2016)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for SDN – Resource control protocols

Signalling requirements for software-defined broadband access network

Recommendation ITU-T Q.3711

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

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

Recommendation ITU-T Q.3711

Signalling requirements for software-defined broadband access network

Summary

Recommendation ITU-T Q.3711 provides an overview of software-defined broadband access network (SBAN) and its procedures, and specifies the signalling requirements of the northbound interface and southbound interface of SBAN model.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3711	2016-08-29	11	11.1002/1000/12989

Keywords

BAN, broadband access network, SDN, software-defined networking.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3711

Signalling requirements for software-defined broadband access network

1 Scope

This Recommendation specifies software-defined broadband access network (SBAN) by providing:

– Overview of SBAN;

– Procedures of SBAN;

– Signalling requirements of the northbound interface and southbound interface of SBAN model;

– Example of SBAN.

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.3300]   Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access network [b-ITU-T Q.1742.11]: Network that connects access technologies such as a radio access network to the core network.

3.1.2 software-defined networking [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APP   Application

APP-ASQ   SDN Application Status Query

APP-ASQP   SDN Application Status Query Response

APP-RE   SDN Application Register

APP-REP   SDN Application Register Response

|	
BAN	Broadband Access Network
BTS	Base Transceiver Station
CE	Customer Edge
eNodeB	Evolved Node B
ID	Identification
IP	Internet Protocol
MAC	Media Access Control
MPLS	Multi-Protocol Label Switching
OAM	Operation, Administration and Maintenance
OPEX	Operating Expense
QoS	Quality of Service
RAN	Radio Access Network
RNC	Radio Network Controller
SBAN	Software-defined Broadband Access Network
SBAN-FI	SBAN Flow Initiation
SBAN-FIP	SBAN Flow Initiation Response
SBAN-FQ	SBAN Flow Query
SBAN-FQP	SBAN Flow Query Response
SBAN-NQ	SBAN Network Query
SBAN-NQP	SBAN Network Query Response
SBAN-NSI	SBAN Network Service Initiation
SBAN-NSIP	SBAN Network Service Initiation Response
SBAN-NSQ	SBAN Network Service Query
SBAN-NSQP	SBAN Network Service Query Response
SBAN-PR	SBAN Node Port Register
SBAN-PRP	SBAN Node Port Register Response
SBAN-PSQ	SBAN Node Port Status Query
SBAN-PSQP	SBAN Node Port Status Query Response
SBAN-RE	SBAN Node Register
SBAN-REP	SBAN Node Register Response
SBAN-SQ	SBAN Node Status Query
SBAN-SQP	SBAN Node Status Query Response
SCTP	Stream Control Transmission Protocol
SDN	Software-Defined Networking
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

| XML | Extensible Markup Language |

5 Conventions

In this Recommendation:

– {A}: indicates that the parameter A is mandatory;
– [B]: indicates that the parameter B is optional;
– *: indicates that the parameter may be multiple items.

6 Introduction of SBAN

Broadband business has become the main source of revenue for carriers, and broadband access network (BAN) plays an important role in carriers' network. But there are still a number of challenges which need to be addressed in BAN, especially for IP radio access network (RAN), see Appendix I.

BAN includes two types of nodes: access nodes and aggregate nodes. The access nodes connect the user devices, such as: base transceiver station (BTS), evolved node B (eNodeB), or customer edge (CE), and the aggregate nodes connect the network devices, such as radio network controller (RNC), the IP metropolitan area network nodes or the IP backbone network nodes. The network topology between access nodes and aggregate nodes can be ring, chain or tree structure. Taking IP RAN for example, IP RAN usually uses a ring structure for network robustness, which is depicted in Figure 6-1.
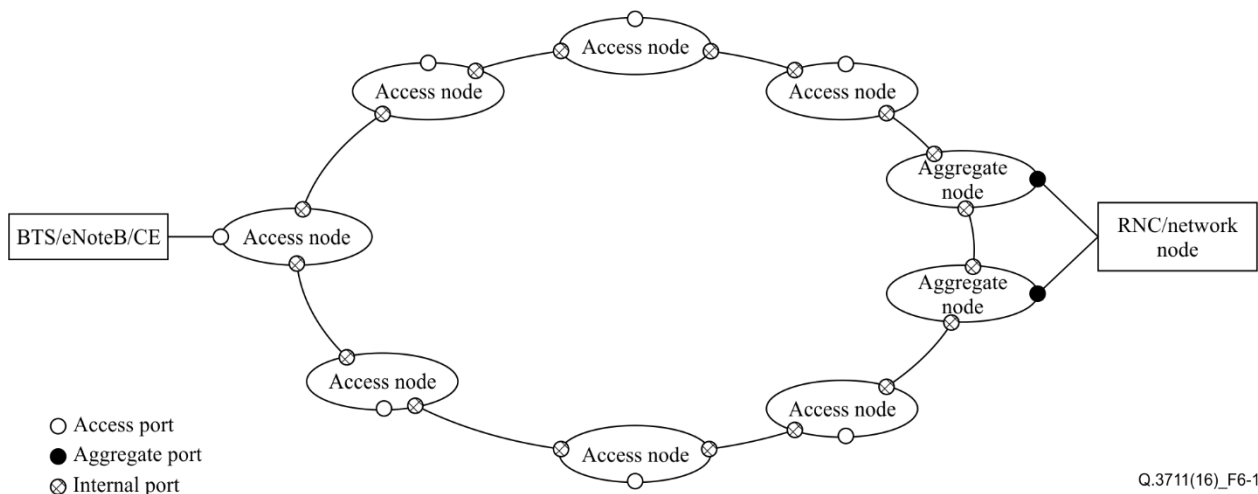
Figure 6-1 – Ring structure of BAN

In Figure 6-1, access ports belong to access nodes that connect user devices, and aggregate ports belong to aggregate nodes that connect other network nodes. Within access nodes and aggregate nodes, there are internal ports that connect to other access nodes or other aggregate nodes.

There are a lot of network equipment and multiple protocols in BAN, and the network topology of BAN is complicated, so network deployment and configuration of BAN requires complex implementation and high maintenance costs. On the other hand, new value-added services and applications emerge rapidly, but it takes weeks or even months for networks to incorporate them.

According to the above, SBAN aims to enable to separate the forwarding function and control function of network equipment, and to provide an open interface to applications and network managers.

The functional entities of the SBAN model consist of forwarding devices, SDN controller, SDN application, southbound interface and northbound interface. Considering the large number of access

nodes, there is a difference between SBAN and other SDN scenarios. It is difficult for the SDN controller in SBAN to link all forwarding devices directly, especially for all access nodes. So in SBAN, the SDN controller only links the aggregate nodes, and abstracts the aggregate nodes and the access nodes as a single node composed of access ports and aggregate ports, which is called an SBAN node and depicted in Figure 6-2.
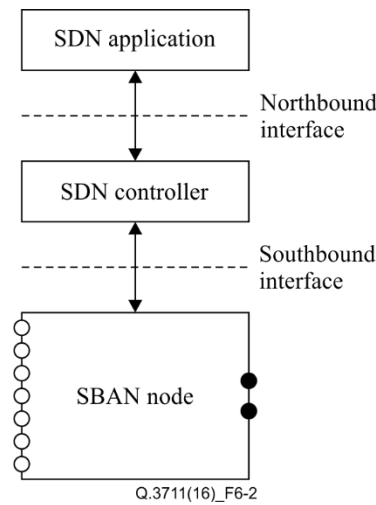
Figure 6-2 – SBAN model

SBAN significantly contributes to reducing operating expense (OPEX) by 1) elimination of both constant maintenance and upgrades to the network equipment; 2) easy deployment of new services; and 3) improvement of the service provisioning.

In SBAN, SBAN nodes perform the actions made by the SDN controller. The SDN controller provides SBAN capabilities to applications and controls SBAN nodes to meet SDN applications' requirements.

The southbound interface is the interface between the SBAN nodes and the SDN controller, which carry messages from the SBAN nodes to the SDN controller (e.g., the link status message) and messages from the SDN controller to the SBAN nodes (e.g., the quality of service (QoS) policy).

The northbound interface is the interface between the SDN controller and the SDN applications, which carries messages from the SDN controller to the SDN application (e.g., the network status message) and messages from the SDN application to the SDN controller (e.g., the network service query).

7 Procedures

7.1 SBAN node initialization

First, the access nodes and the aggregate nodes are initialized without the SDN controller. The access nodes send their information to the aggregate nodes through the internal interface, such as: manufacturer identification, equipment models, media access control (MAC) address, access ports, internal ports. The aggregate nodes collect the information from the access nodes or the other aggregate nodes in the same network.

Then the aggregate nodes negotiate with each other to elect the master aggregate node and the slave aggregate nodes. The master aggregate node communicates on behalf of the SBAN node with the SDN controller, as depicted in Figure 7-1.
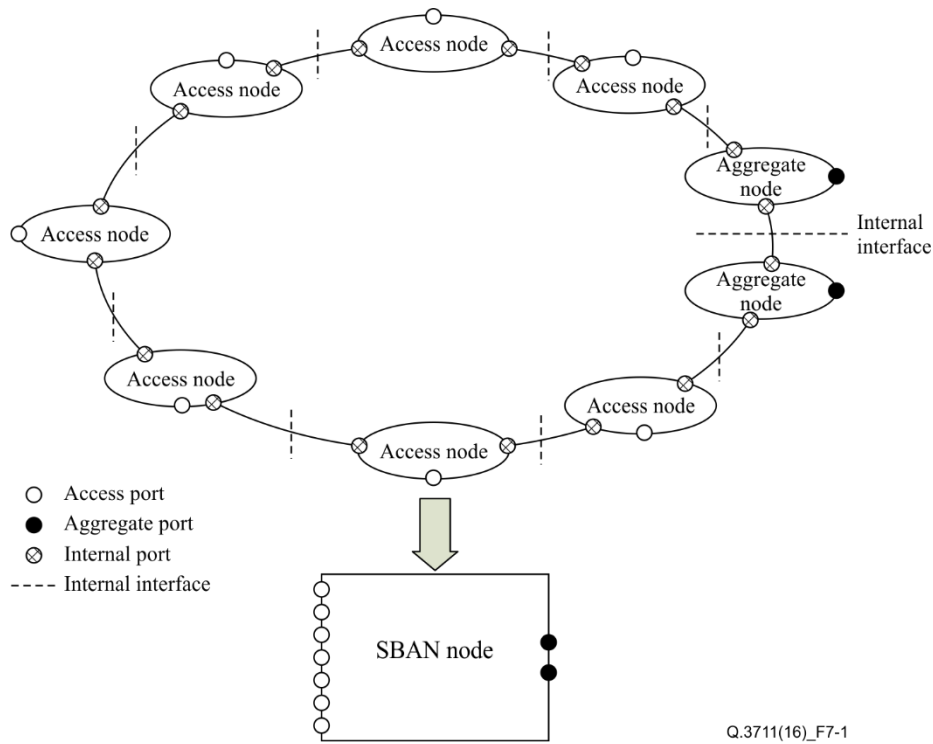
Figure 7-1 – SBAN node initialization

The master aggregate node has all the information about the access ports and the aggregate ports, and synchronizes with the slave aggregate nodes. When the master aggregate node fails, one of the slave aggregate nodes will become the new master aggregate node which represents the SBAN nodes to maintain communication with the SDN controller.

The internal interface between the aggregate nodes and the access nodes is not included in this Recommendation.

7.2 Registration

After the SBAN node finishes its initialization, the master aggregate node is registered in the SDN controller as the representation of the SBAN node. In this process, the master aggregate node announces its information to the SDN controller, such as: address information, the slave aggregate nodes information. The SDN controller responds with the registration information, and allocates an SBAN node identification (ID) to the master aggregate node.

The master aggregate node registers all the ports, including the access ports and the aggregate ports of the SBAN node, by using the SBAN node ID in the SDN controller.

Meanwhile, the SDN application is registered in the SDN controller.

7.3 Status query

After the SBAN node and the SDN application are registered in the SDN controller, the SDN controller queries the their status. And the SDN application queries the topology and abilities of the SBAN nodes through the SDN controller.

7.4 Service creation

The SDN application initiates the network service of the SBAN nodes, and the SDN controller receives and translates the initiation. Then the SDN controller initiates the flows in the SBAN nodes.

8 The signalling requirements of SBAN

8.1 Overview of signalling requirements

For controlling the SBAN network, the messages over the southbound interface and the northbound interface are classified by the following three categories.

Category 1: Registration

1-1   (southbound) SBAN Node Register message and response message;

1-2   (southbound) SBAN Node Port Register message and response message;

1-3   (northbound) SDN application Register message and response message.

Category 2: Status query

2-1   (southbound) SBAN Node Status Query message and response message;

2-2   (southbound) SBAN Node Port Status Query message and response message;

2-3   (southbound) SBAN Flow Query message and response message;

2-4   (northbound) SDN application Status Query message and response message;

2-5   (northbound) SBAN Network Query message and response message;

2-6   (northbound) SBAN Network Service Query message and response message.

Category 3: Service creation

3-1   (northbound) SBAN Network Service Initiation message and response message;

3-2   (southbound) SBAN Flow Initiation message and response message.

NOTE – No transport protocol for the signalling messages is specified here. No message content format is specified here either.

The signalling messages may be extensible markup language (XML)-based messages over (or carried by) transmission control protocol (TCP), user datagram protocol (UDP), stream control transmission protocol (SCTP), transport layer security (TLS), etc. All of the messages consist of the message header and the message body.

The message format is described in Figure 8-1 as follows:
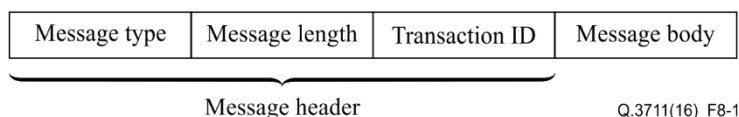
Figure 8-1 – Message composition

The message header field contains the following information:

1)   Message type: uniquely specifies the type of message;

2)   Message length: specifies the length of the message body;

3)   Message transaction ID: generated by the sender of the message. If there is a response message for the request message, the transaction IDs of the request and response messages are the same.

The message body field contains the message contents.

8.2 Signalling requirements for southbound interface

8.2.1 Signalling requirements for registration

8.2.1.1 SBAN Node Register message and response message

The SBAN Node Register message is defined as SBAN-RE message.

The SBAN-RE message, indicated by the message type in the message header field, is sent by the master aggregate node to be registered in the SDN controller.

Message format:

```
< SBAN-RE-Message > ::= < Message header >
                { SDN-controller-Address }
                { Master-Aggregate-node-Address }
              *{ Slave-Aggregate-node-Address }
              *{ SBAN-node-Attribute }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `Master-Aggregate-node-Address` uniquely specifies the master aggregate node;

3)   `Slave-Aggregate-node-Address` uniquely specifies the slave aggregate node. There may be multiple slave aggregate nodes;

4)   `SBAN-node-Attribute` is used for the aggregate node attributes. There may be multiple node attribute items.

The response message to the SBAN-RE message is defined as SBAN-REP message.

The SBAN-REP message, indicated by the message type in the message header field, is sent by the SDN controller to the master aggregate node in response to the SBAN-RE message.

Message format:

```
< SBAN-REP-Message> ::= < Message Header >
                { SDN-controller-Address }
                { Master-Aggregate-node-Address }
                { SBAN-node-ID }
                { Result }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `Master-Aggregate-node-Address` uniquely specifies the master aggregate node, which may be renamed as `SBAN-node-Address` when the master aggregate node represents SBAN node;

3)   `SBAN-node-ID` uniquely specifies the SBAN node, which is assigned by the SDN controller and is globally validated. After the SBAN node has registered successfully, this ID is used in subsequent messages, including the messages from the SDN controller to the SBAN node and from the SBAN node to the SDN controller;

4)   `Result` shows the handling results of registering the SBAN node in the SDN controller.

8.2.1.2 SBAN Node Port Register message and response message

The port information of the SBAN Node Port Register message is defined as SBAN-PR message.

The SBAN-PR message, indicated by the message type in the message header field, is sent by the master aggregate node to be registered in the SDN controller.

Message format:

```
< SBAN-PR-Message > ::= < Message header >
              { SDN-controller-Address }
              { SBAN-node-Address }
              { SBAN-node-ID }
             *{ Port-ID }
            *{ Port-Type-ID }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;
2)   `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;
3)   `SBAN-node-ID` uniquely specifies the SBAN node;
4)   `Port-ID` uniquely specifies the port of the SBAN node;
5)   `Port-Type-ID` uniquely specifies the type of the port, such as access port or aggregate port.

The response message to the SBAN-PR message is defined as SBAN-PRP message.

The SBAN-PRP message, indicated by the message type in the message header field, is sent by the SDN controller to the SBAN node, which is represented by the master aggregate node, in response to the SBAN-PR message.

Message format:

```
< SBAN-PRP-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SBAN-node-Address }
              { SBAN-node-ID }
              { Result }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;
2)   `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;
3)   `SBAN-node-ID` uniquely specifies the SBAN node;
4)   `Result` shows the handling results of registering the ports in the SDN controller.

8.2.2   Signalling requirements for status query

8.2.2.1   SBAN Node Status Query message and response message

The SBAN node status request message is defined as SBAN-SQ message.

The SBAN-SQ message, indicated by the message type in the message header field, is sent by the SDN controller to the master aggregate node in order to get the node status of the SBAN node.

Message format:

```
<SBAN-SQ-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SBAN-node-Address }
              { SBAN-node-ID }
            *{ Node-Type-ID }
            *[ Node-Parameter-ID ]
            *[ Auto-Node-ID ]
            *[ Auto-Node-Parameter-ID ]
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;

3) `SBAN-node-ID` uniquely specifies the SBAN node;

4) `Node-Type-ID` uniquely specifies the type of status enquired by the SDN controller;

5) `Node-Parameter-ID` is optional, some of the status may need this ID to specify the intended status. One possible example would be the port number (or ID) of the designated port;

6) `Auto-Node-ID` and `Auto-Node-Parameter-ID` are optional and have the same meaning with item 4 and item 5, respectively. The auto here means the aggregate node will automatically report the specified status to the SDN controller in case of changes.

The SBAN node status response message is defined as SBAN-SQP message.

The SBAN-SQP message, indicated by the message type in the message header field, is sent by the master aggregate node to the SDN controller in response to the SBAN-SQ message.

Message format:

```
<SBAN-SQP-Message> ::= < Message Header >
               { SDN-controller-Address }
               { SBAN-node-Address }
               { SBAN-node-ID }
             *{ Node-Type-ID }
             *[ Node-Parameter-ID ]
             *{ Node-Status-Value }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SBAN-node-Address` uniquely specifies the SBAN node address, which is equal to `Master-Aggregate-node-Address`;

3) `SBAN-node-ID` uniquely specifies the SBAN node;

4) `Node-Type-ID` uniquely specifies the type of status enquired by the SDN controller;

5) `Node-Parameter-ID` is optional, some of the status may need this ID to specify the intended status. One possible example would be the port number (or ID) of the designated port;

6) `Node-Status-Value` is used for describing the status of the SBAN node specified by `Node-Type-ID`.

8.2.2.2 SBAN Node Port Status Query message and response message

The SBAN node status request message is defined as SBAN-PSQ message.

The SBAN-PSQ message, indicated by the message type in the message header field, is sent by the SDN controller to the master aggregate node in order to get the port status of the SBAN node.

Message format:

```
<SBAN-PSQ-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SBAN-node-Address }
              { SBAN-node-ID }
             { Port-ID }
            *{ Port-Type-ID }
            *[ Port-Parameter-ID ]
            *[ Auto-Port-ID ]
            *[ Auto-Port-Parameter-ID ]
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;
2)   `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;
3)   `SBAN-node-ID` uniquely specifies the SBAN node;
4)   `Port-ID` uniquely specifies the port of the SBAN node;
5)   `Port-Type-ID` uniquely specifies the type of the port enquired by the SDN controller;
6)   `Port-Parameter-ID` is optional, some of the status may need this ID to specify the intended status;
7)   `Auto-Port-ID` and `Auto-Port-Parameter-ID` are optional and have the same meaning with item 5 and item 6, respectively. The auto here means the SBAN node will automatically report the specified status to the SDN controller in case of changes.

The SBAN node status response message is defined as SBAN-PSQP message.

The SBAN-PSQP message, indicated by the message type in the message header field, is sent by the master aggregate node to the SDN controller in response to the SBAN-PSQ message.

Message format:

```
<SBAN-PSQP-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SBAN-node-Address }
              { SBAN-node-ID }
             { Port-ID }
            *{ Port-Type-ID }
            *[ Port-Parameter-ID ]
            *{ Port-Status-Value }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;

3)   `SBAN-node-ID` uniquely specifies the SBAN node;

4)   `Port-ID` uniquely specifies the port of the SBAN node;

5)   `Port-Type-ID` uniquely specifies the type of the port enquired by the SDN controller;

6)   `Port-Parameter-ID` is optional, some of the status may need this ID to specify the intended status;

7)   `Port-Status-Value` is used for describing the status of the port specified by `Port-ID`.

8.2.2.3   SBAN Flow Query message and response message

The SBAN Flow Query message is defined as SBAN-FQ message.

The SBAN-FQ message, indicated by the message type in the message header field, is sent by the SDN controller to the master aggregate node in order to get the flow information of the SBAN node.

Message format:

```
<SBAN-FQ-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SBAN-node-Address }
                { SBAN-node-ID }
              *{ Flow-ID }
              *[ Flow-Parameter-ID ]
              *[ Auto-Flow-ID ]
              *[ Auto-Flow-Parameter-ID ]
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;

3)   `SBAN-node-ID` uniquely specifies the SBAN node;

4)   `Flow-ID` uniquely specifies the flow enquired by the SDN controller;

5)   `Flow-Parameter-ID` is optional, some of the status may need this ID to specify the intended status;

6)   `Auto-Flow-ID` and `Auto-Flow-Parameter-ID` are optional and have the same meaning with item 4 and item 5, respectively. The auto here means the aggregate node will automatically report the specified status to the SDN controller in case of changes.

The SBAN Flow Query response message is defined as SBAN-FQP message.

The SBAN-FQP message, indicated by the message type in the message header field, is sent by the master aggregate node to the SDN controller in response to the SBAN-FQ message.

Message format:

```
<SBAN-FQP-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SBAN-node-Address }
                { SBAN-node-ID }
              *{ Flow-ID }
              *[ Flow-Parameter-ID ]
              *{ Flow-Status-Value }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;

3) `SBAN-node-ID` uniquely specifies the SBAN node;

4) `Flow-ID` uniquely specifies the flow enquired by the SDN controller;

5) `Flow-Parameter-ID` is optional; some of the flow may need this ID to specify the intended status;

6) `Flow-Status-Value` is used for describing the status of the flow specified by `Flow-ID`.

8.2.3 Signalling requirements for service creation

8.2.3.1 SBAN Flow Initiation message and response message

The SBAN Flow Initiation message is defined as SBAN-FI message.

The SBAN-FI message, indicated by the message type in the message header field, is sent by the SDN controller to the aggregate node in order to initiate the flow in the SBAN node.

Message format:

```
<SBAN-FI-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SBAN-node-Address }
                { SBAN-node-ID }
                { Port-ID }
              *{ Flow-ID }
              *[ Flow-Parameter-ID ]
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SBAN-node-Address` uniquely specifies the SBAN node address, which may be equal to `Master-Aggregate-node-Address`;

3) `SBAN-node-ID` uniquely specifies the SBAN node;

4) `Port-ID` uniquely specifies the port of the SBAN node;

5) `Flow-ID` uniquely specifies the flow sent by the SDN controller;

6) `Flow-Parameter-ID` is optional; some of the parameter status may need this ID to specify the intended flow status.

The SBAN Flow Initiation response message is defined as SBAN-FIP message.

The SBAN-FIP message, indicated by the message type in the message header field, is sent by the master aggregate node to the SDN controller in response to the SBAN-FI message.

Message format:

```
<SBAN-FIP-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SBAN-node-Address }
                { SBAN-node-ID }
               *{ Flow-ID }
               *[ Flow-Parameter-ID ]
               *{ Flow-Status-Value }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SBAN-node-Address` uniquely specifies the SBAN node address, which is equal to `Master-Aggregate-node-Address`;

3) `SBAN-node-ID` uniquely specifies the SBAN node;

4) `Flow-ID` uniquely specifies the flow sent by the SDN controller;

5) `Flow-Parameter-ID` is optional, some of the status may need this ID to specify the intended status;

6) `Flow-Status-Value` is used for describing the status of the flow specified by `Flow-ID`.

8.3 Signalling requirements for northbound interface

8.3.1 Signalling requirements for registration

8.3.1.1 SDN application Register message and response message

The SDN application Register message is defined as APP-RE message.

The APP-RE message, indicated by the message type in the message header field, is sent by the SDN application to be registered in the SDN controller.

Message format:

```
< APP-RE-Message > ::= < Message header >
                { SDN-controller-Address }
                { SDN-application-Address }
                { SDN-application-ID }
               *{ SDN-application-Attribute-ID }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SDN-application-Address` uniquely assigned to the SDN application;

3) `SDN-application-ID` uniquely specifies the SDN application;

4) `SDN-application-Attribute-ID` is used for the SDN application attributes. There may be multiple SDN application attribute items.

The response message to the APP-RE message is defined APP-REP message.

The APP-REP message, indicated by the message type in the message header field, is sent by the SDN controller to the SDN application in response to the APP-RE message.

Message format:

```
< APP-REP-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SDN-application-Address }
              { SDN-application-ID }
              { Result }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SDN-application-Address` uniquely assigned to the SDN application;

3) `SDN-application-ID` uniquely specifies the SDN application;

4) `Result` shows the handling results of registering the SDN application in the SDN controller.

8.3.2 Signalling requirements for querying status

8.3.2.1 SDN application Status Query message and response message

The SDN application Status Query message is defined as APP-ASQ message.

The APP-ASQ message, indicated by the message type in the message header field, is sent by the SDN controller to the SDN application in order to get the status of the SDN application.

Message format:

```
<APP-ASQ-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SDN-application-Address }
              { SDN-application-ID }
            *{ SDN-application-Attribute-ID }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2) `SDN-application-Address` uniquely assigned to the SDN application;

3) `SDN-application-ID` uniquely specifies the SDN application;

4) `SDN-application-Attribute-ID` is used for the SDN application attributes. There may be multiple SDN application attribute items.

The SDN application Status Query response message is defined as APP-ASQP message.

The APP-ASQP message, indicated by the message type in the message header field, is sent by the SDN application to the SDN controller in response to the APP-ASQ message.

Message format:

```
<APP-ASQP-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SDN-application-Address }
              { SDN-application-ID }
            *{ SDN-application-Attribute-ID }
            *{ SDN-application-Status-Value }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `SDN-application-Address` uniquely assigned to the SDN application;

3)   `SDN-application-ID` uniquely specifies the SDN application;

4)   `SDN-application-Attribute-ID` is used for the SDN application attributes. There may be multiple SDN application attribute items;

5)   `SDN-application-Status-Value` is used for describing the status of the SDN application specified by `SDN-application-Attribute-ID`.

8.3.2.2 SBAN Network Query message and response message

The SBAN network status request message is defined as SBAN-NQ message.

The SBAN-NQ message, indicated by the message type in the message header field, is sent by the SDN application to the SDN controller in order to get the network status of the SBAN.

Message format:

```
<SBAN-NQ-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SDN-application-Address }
            { SDN-application-ID }
            *{ Network-ID }
            *[ Auto-Network-ID ]
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `SDN-application-Address` uniquely assigned to the SDN application;

3)   `SDN-application-ID` uniquely specifies the SDN application;

4)   `Network-ID` uniquely specifies the network enquired by the SDN application;

5)   `Auto-Network-ID` is optional and has the same meaning with item 4. The auto here means the SDN controller will automatically report the specified network status in case of changes.

The SBAN network status response message is defined as SBAN-NQP message.

The SBAN-NQP message, indicated by the message type in the message header field, is sent by the SDN controller to the SDN application in response to the SBAN-NQ message.

Message format:

```
<SBAN-NQP-Message> ::= < Message Header >
              { SDN-controller-Address }
              { SDN-application-Address }
              { SDN-application-ID }
            *{ Network-ID }
            *{ Network-Status-Value }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;

2)   `SDN-application-Address` uniquely assigned to the SDN application;

3)   `SDN-application-ID` uniquely specifies the SDN application;

4)   `Network-ID` uniquely specifies the network enquired by the SDN application;

5) `Network-Status-Value` is used for describing the status of the SBAN network specified by `Network-Type-ID`.

8.3.2.3 SBAN Network Service Query message and response message

The SBAN Network Service Query message is defined as SBAN-NSQ message.

The SBAN-NSQ message, indicated by the message type in the message header field, is sent by the SDN application to the SDN controller in order to get the network service status of the SBAN.

Message format:

```
<SBAN-NSQ-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SDN-application-Address }
                { SDN-application-ID }
              *{ Network-Service-ID }
              *[ Auto-Services-ID ]
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;
2) `SDN-application-Address` uniquely assigned to the SDN application;
3) `SDN-application-ID` uniquely specifies the SDN application;
4) `Network-Service-ID` uniquely specifies network service enquired by the SDN application;
5) `Auto-Services-ID` is optional and has the same meaning with item 4. The auto here means the SDN controller will automatically report the specified service status in case of changes.

The network service status response message is defined as SBAN-NSQP message.

The SBAN-NSQP message, indicated by the message type in the message header field, is sent by the SDN controller to the SDN application in response to the SBAN-NSQ message.

Message format:

```
<SBAN-NSQP-Message> ::= < Message Header >
                { SDN-controller-Address }
                { SDN-application-Address }
                { SDN-application-ID }
              *{ Network-Service-ID }
              *{ Services-Status-Value }
```

Meanings and explanations:

1) `SDN-controller-Address` uniquely specifies the SDN controller;
2) `SDN-application-Address` uniquely assigned to the SDN application;
3) `SDN-application-ID` uniquely specifies the SDN application;
4) `Network-Service-ID` uniquely specifies the network service enquired by the SDN application;
5) `Services-Status-Value` is used for describing the service status specified by `Services-ID`.

8.3.3 Signalling requirements for service creation

8.3.3.1 SBAN Network Service Initiation message and response message

The SBAN Network Service Initiation message is defined as SBAN-NSI message.

The SBAN-NSI message, indicated by the message type in the message header field, is sent by the SDN application to the SDN controller in order to initiate the network service in the SBAN network.

Message format:

```
<SBAN-NSI-Message> ::= < Message Header >
             { SDN-controller-Address }
             { SDN-application-Address }
             { SDN-application-ID }
           *{ Network-service-ID }
           *[ Network-service-Parameter-ID ]
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;
2)   `SDN-application-Address` uniquely assigned to the SDN application;
3)   `SDN-application-ID` uniquely specifies the SDN application;
4)   `Network-service-ID` uniquely specifies the network service sent by the SDN application;
5)   `Network-service-Parameter-ID` is optional; some of the parameter status may need this ID to specify the intended network service status.

The SBAN Network Service Initiation response message is defined as SBAN-NSIP message.

The SBAN-NSIP message, indicated by the message type in the message header field, is sent by the SDN controller to the SDN application in response to the SBAN-NSI message.

Message format:

```
<SBAN-NSIP-Message> ::= < Message Header >
             { SDN-controller-Address }
             { SDN-application-Address }
             { SDN-application-ID }
           *{ Network-service-ID }
           *[ Network-service-Parameter-ID ]
           *{ Network-service-Status-Value }
```

Meanings and explanations:

1)   `SDN-controller-Address` uniquely specifies the SDN controller;
2)   `SDN-application-Address` uniquely assigned to the SDN application;
3)   `SDN-application-ID` uniquely specifies the SDN application;
4)   `Network-service-ID` uniquely specifies the network service sent by the SDN application;
5)   `Network-service-Parameter-ID` is optional, some of the status may need this ID to specify the intended status;
6)   `Network-service-Status-Value` is used for describing the status of the network service specified by `Network-service-ID`.

9 Security considerations

The SBAN includes the forwarding function (i.e., SBAN nodes), the control function (i.e., SDN controller) of network equipment and SDN applications, similar to the other SDN scenarios. SBAN follows the security consideration in [ITU-T Y.3300].

Appendix I

An example of SBAN

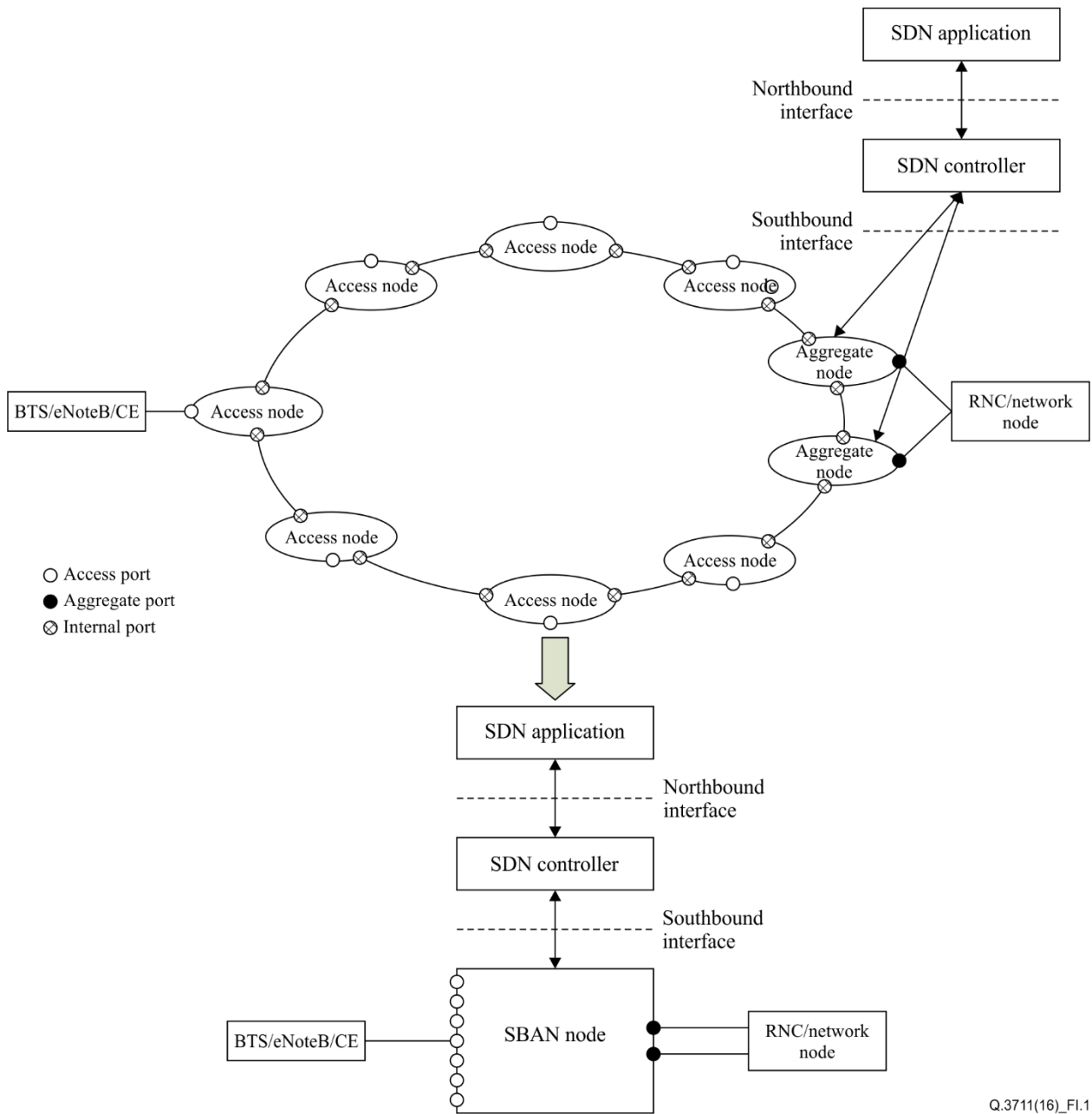(This appendix does not form an integral part of this Recommendation.)

IP RAN is based on IP/multi-protocol label switching (MPLS) technology framework, through enhanced operation, administration and maintenance (OAM), protection, clock, network management and other capabilities, to meet the needs of wireless, access and other integrated services.

Compared with other IP network, IP RAN has the following characteristics:

1)   IP RAN has only two kinds of topology: ring or chain structure. In most cases, it will be ring structure due to network robustness;

2)   An access node only belongs to a ring or a chain;

3)   One endpoint of the flow in the IP RAN is an access port, the other side is an aggregate port or an access port in the same ring or the same chain;

4)   Based on the ring structure, the work and backup path of each flow have only two options: clockwise or counter clockwise.

Each ring or chain can be abstracted into a simple virtual switch which composed of access ports and aggregate ports, without considering the specific path.

In software-defined IP RAN, each ring or chain can be abstracted into a virtual SDN switch composed of access ports and aggregate ports, which is called SBAN node and depicted in Figure I.1.

Figure I.1 – SBAN node in software-defined IP RAN

Bibliography

[b-ITU-T Q.1742.11]   Recommendation ITU-T Q.1742.11 (2014), *IMT 2000 references (approved as of 31st December 2012) to ANSI-41-evolved core network with cdma2000 access network.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	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	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems