Messages for certificate installation and retrieval

version 5

G. Kramer

Current solution in D2.2

- Two new OAMPDU types are defined for managing certificates
- Action codes are defined to
  - 0x00 - Install NAC (or chain)
  - 0x01 - Retrieve DAC
  - 0x02 - Retrieve NAC (or chain)

Table 13-10—eOAMPDUs and assignment of Opcode values

Opcode	eOAMPDUs	Defined in
0x01	*eOAM_Get_Request*	13.4.6.2
0x02	*eOAM_Get_Response*	13.4.6.3
0x03	*eOAM_Set_Request*	13.4.6.4
0x04	*eOAM_Set_Response*	13.4.6.5
0x09	*eOAM_Software*	13.4.6.6
0x0A	*eOAM_Certificate_Request*	13.4.6.7
0x0B	*eOAM_Certificate_Response*	13.4.6.7

Install NAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	Action Code	0x00
2	Certificate Length	The length of the Certificate field. The value of 0x00 indicates that this is a request to remove the existing NAC certificate
≤ 1489	Certificate Data	NAC certificate data. This field is not present if the `CertificateLength` is 0x00.
≤ 35	Pad	
4	FCS	

Install NAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	Action Code	0x00
1	Action Status	Value encoding the status of a taken/attempted action, as defined in Table 13-24
1	Certificate Status	Value encoding the status of the installed certificate, as defined in Table 13-25
35	Pad	0x00-…-00
4	FCS	

Retrieve NAC/DAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	Action Code	`0x01`: retrieve the DAC `0x02`: retrieve the NAC.
37	Pad	0x00-…-00
4	FCS	

Retrieve NAC/DAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	Action Code	`0x01`: DAC certificate `0x02`: NAC certificate
2	Certificate Length	The length of the Certificate field. The value of 0x00 indicates that the requested certificate (NAC or DAC) is not present or cannot be retrieved.
≤ 1489	Certificate Data	DAC or NAC certificate data. This field is not present if the `CertificateLength` is 0x00.
≤ 35	Pad	
4	FCS	See 13.4.2

If NAC comes with intermediate certificates, the entire certificate chain must fit within this field

Install/Replace NAC

- ACK or NACK after every request OAMPDU
- How long should ONU wait for the next block? What to do if the next block doesn't arrive?
- Should we allow the OLT to send several blocks back-to-back and then wait for that number of ACKs?

Action	ActionCode value
Install NAC	0xA1
Delete NAC	0xD1
Retrieve NAC	0x01
Retrieve DAC	0x00

Install/Replace NAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	ActionCode	0xA1
4	Sequence	Bit 31: `Start` indicator (1) Bits 30-0: `ResidualOctets` = number of the remaining certificate data octets, not counting the octets in the `BlockData` field.
2	BlockLength	The length of the `BlockData` field.
≤ 1485	DataBlock	A block of NAC certificate data. This field is not present if the `BlockLength` is 0x00.
≤ 31	Pad	0x00-…-00
4	FCS	

Install/Replace NAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	ActionCode	0xA1
4	Sequence	Bit 31: copy of bit 31 from request Bits 30-0: `ResidualOctets`. ONU acknowledges that it received all certificate octets except the remaining `ResidualOctets`.
1	ActionStatus	Value encoding the status of a taken/attempted action, as defined in Table 13-24. This field is only present if `ResidualOctets = 0x00-00-00-00`
1	Certificate Status	Value encoding the status of the installed certificate, as defined in Table 13-25. This field is only present if `ResidualOctets = 0x00-00-00-00`
31 or 33	Pad	0x00-…-00
4	FCS	

- When the ONU receives OLT's request with **`ResidualOctets = N`**, it generates the response with **`ResidualOctets = N`**
- When the OLT receives ONU's response with **`ResidualOctets = N`**, it generates the next request with **`ResidualOctets = N - BlockLength`**
- If case of ONU response timeout, the OLT resends the last request.

Delete NAC – 2 options

Dedicated **ActionCode** for Delete NAC

Action	ActionCode value
Install NAC	0xA1
Delete NAC	0xD1
Retrieve NAC	0x01
Retrieve DAC	0x00

Delete NAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	ActionCode	0xD1
37	Pad	0x00-…-00
4	FCS	

This option introduces 2 new message formats with new parsing rules

Delete NAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	ActionCode	0xD1
1	ActionStatus	Value encoding the status of a taken/attempted action, as defined in Table 13-24.
1	CertificateStatus	Value encoding the status of the installed certificate, as defined in Table 13-25.
33	Pad	0x00-…-00
4	FCS	

Delete NAC == Install zero-length NAC

Action	ActionCode value
Install NAC	0xA1
Retrieve NAC	0x01
Retrieve DAC	0x00

Delete NAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	ActionCode	0xA1
4	Sequence	0x80-00-00-00
2	BlockLength	0x00-00
31	Pad	0x00-…-00
4	FCS	

Delete NAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	ActionCode	0xA1
4	Sequence	0x80-00-00-00
1	ActionStatus	
1	CertificateStatus	
31	Pad	0x00-…-00
4	FCS	

Retrieve DAC/NAC

- ACK or NACK after every request OAMPDU
- If the OLT decides to abort the retrieval, how is this signaled to the ONU?

Action	`ActionCode` value
Install NAC	0xA1
Delete NAC	0xD1
Retrieve NAC	0x01
Retrieve DAC	0x00

Retrieve NAC/DAC (request)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0A
1	ActionCode	`0x00`: retrieve the DAC `0x01`: retrieve the NAC
4	Sequence	Bit 31: `Start` indicator (1) Bits 30-0: `ReceivedOctets` = OLT requests the ONU to send the next block that starts at octet index `ReceivedOctets`
37	Pad	0x00-…-00
4	FCS	

Note, this is **`ReceivedOctets`**, not **`ResidualOctets`**
In the initial request,
`Sequence = 0x80-00-00-00`

Retrieve NAC/DAC (response)

Size (B)	Field name	Value and notes
21	eOAMPDU header	See Table 13-2
1	Opcode	0x0B
1	ActionCode	`0x00`: retrieve the DAC `0x01`: retrieve the NAC
4	Sequence	Bit 31: copy of bit 31 from request Bits 30-0: `ResidualOctets` = the number of the remaining certificate data octets, not counting the octets in the `BlockData` field.
2	BlockLength	The length of the `BlockData` field.
≤ 1485	DataBlock	A block of NAC certificate data. This field is not present if the `BlockLength` is 0x00.
≤ 31	Pad	0x00-…-00
4	FCS	

- If the ONU is unable to retrieve the next **`DataBlock`** before the OAM timeout, it sends a message with **`BlockLength = 0`**.
- If OLT receives a response with **`ResidualOctets > 0`** and **`BlockLength == 0`**, it treats it as a "keep alive".
- Keep-alive means that the ONU will transmit the requested block as soon as it can and without another OLT request.
- The could be several keep-alives before the next block becomes available at the ONU.