

Embedded systems course

SMS Protocol specification

Cellular phones send and receive periodic control messages to the nearest antenna.

When a cell phone sends an SMS message, the message is “piggybacking” the control message, and the cell antenna sends it to a central server (SMSC – Short Message Service Center).

When the cell phone that is the destination of the SMS sends a similar control message to its nearest antenna, the SMS message waiting for it in the SMSC is being sent as part of the control message reply.

Description of the real life SMS PDU format can be found at: <http://www.dreamfabric.com/sms/>

The device in this exercise will periodically send an SMS_PROBE control message to the SMSC. If an SMS message is pending for the device, the SMSC will reply with an SMS_DELIVER message.

After receiving an SMS_DELIVER message, the device needs to acknowledge the reception of the SMS message so the SMSC can delete it from its database. This is done by the device sending an SMS_PROBE_ACK message as its next control message.

Besides removing the previous deliver message, the SMSC treat an SMS_PROBE_ACK message as a regular probe message, so it will reply with a new SMS_DELIVER message if there is another SMS message pending for this device.

When the device wants to send an SMS message it sends an SMS_SUBMIT message. The SMSC will reply with an SMS_SUBMIT_ACK if the SMS was successfully added to the server.

You can access the SMSC directly from the web at <http://www.cs.huji.ac.il/~embsys/SMSC.php>, where you can send SMS messages, see the pending messages and the devices that are "alive" in the network.

Devices in the network are identified using a unique address number. This address is made of maximum 8 decimal digits. You should use your personal ID number to prevent conflicts in our network. Address "0" is reserved for the SMSC.

1.1 SMS_PROBE message format

Octet(s)	Description
02	SMS_PROBE
09	Address-Length. Length of the sender number.
C9	Type-of-address of the sender number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Sender number. This value is in decimal semi-octets, with a trailing F for padding. The octets to the left represents subscriber number "123456789"

1.2 SMS_PROBE_ACK message format

Octet(s)	Description
12	SMS_PROBE_ACK
09	Address-Length. Length of the sender number.
C9	Type-of-address of the sender number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Sender number. This value is in decimal semi-octets, with a trailing F for padding.
99 30 92 51 61 95 80	TP-SCTS. Acknowledged SMS Time stamp (semi-octets)
09	Ack-Address-Length. Length of the acknowledged SMS sender number
C9	Ack- Type-of-address of the acknowledged SMS sender number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Acknowledged SMS sender number. This value is in decimal semi-octets, with a trailing F for padding.

1.3 SMS_DELIVER message format

Octet(s)	Description
04	SMS_DELIVER
09	Address-Length. Length of the sender number. A value of zero means no messages are available.
C9	Type-of-address of the sender number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Sender number. This value is in decimal semi-octets, with a trailing F for padding.
00	TP-PID. Protocol identifier .
00	TP-DCS. Data coding scheme . This message is coded according to the 7bit alphabet.
99 30 92 51 61 95 80	TP-SCTS. Time stamp (semi-octets)
0A	TP-UDL. User data length, length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10).
E8329BFD4697D9EC37	TP-User-Data. These octets represent the message "hellohello". How to do the transformation from 7bit septets into octets is shown here

1.4 SMS_SUBMIT message format

Octet(s)	Description
11	SMS_SUBMIT
09	Address-Length. Length of the sender number.
C9	Type-of-address of the sender number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Sender number. This value is in decimal semi-octets, with a trailing F for padding.
00	TP-Message-Reference. This value is used to uniquely identify the submitted message, so the corresponding SMS_SUBMIT_ACK can be matched.
09	Address-Length. Length of the recipient number.
C9	Type-of-address of the recipient number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Recipient number. This value is in decimal semi-octets, with a trailing F for padding.
00	TP-PID. Protocol identifier
00	TP-DCS. Data coding scheme . This message is coded according to the 7bit alphabet.
3B	TP-Validity-Period . The SMSC ignores this values and always use "3B" .
0A	TP-User-Data-Length. Length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10).
E8329BFD4697D9EC37	TP-User-Data. These octets represent the message "hellohello". How to do the transformation from 7bit septets into octets is shown here

1.5 SMS_SUBMIT_ACK message format

Octet(s)	Description
07	SMS_SUBMIT_ACK
00	TP-Message-Reference. This value equals to the one used in the SMS_SUBMIT message that is being acknowledged by this SMS_SUBMIT_ACK message.
09	Address-Length. Length of the recipient number.
C9	Type-of-address of the recipient number. Always use Subscriber number type with Private numbering plan.
21 43 65 87 F9	Recipient number. This value is in decimal semi-octets, with a trailing F for padding. The octets to the left represents subscriber number "123456789"