

Robotics Service Bus - Bug #1173

Socket server dies because of incomplete message body

09/20/2012 03:15 PM - J. Wienke

Status:	Resolved	Start date:	09/20/2012
Priority:	High	Due date:	
Assignee:	J. Moringen	% Done:	0%
Category:	C++	Estimated time:	0.00 hour
Target version:	rsb-0.7		

Description

NAO is sending images and a program

```
humavips@HUMAVIPS:~/work$ ~/work/RSB-0.7/bin/rsb_videoreceiver
```

```
1348146353274 rsb.transport.socket.BusServer [WARN]: Send failure (Connection reset by peer); will close connection later
```

```
1348146353276 rsb.transport.socket.BusServer [WARN]: Send failure (Connection reset by peer); will close connection later
```

```
1348146353280 rsb.transport.socket.BusConnection [WARN]: Receive failure (error asio.misc:2) or incomplete message body (received 25341 bytes); closing connection
```

```
1348146353291 rsb.transport.socket.BusConnection [WARN]: Receive failure (error asio.misc:2) or incomplete message body (received 510 bytes); closing connection
```

Segmentation fault

```
0x00007ffff5c0956b in std::string::assign(std::string const&) () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
```

(gdb) bt

```
#0 0x00007ffff5c0956b in std::string::assign(std::string const&) () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
```

```
#1 0x00007ffff77f8a09 in rsb::protocol::Notification::set_data(std::string const&) () from /usr/lib/librsbcore.so.0.7.3
```

```
#2 0x00007ffff78873d3 in rsb::transport::socket::eventToNotification(rsb::protocol::Notification&, boost::shared_ptr<rsb::Event> const&, std::string const&, std::string const&) () from /usr/lib/librsbcore.so.0.7.3
```

```
#3 0x00007ffff7855e82 in rsb::transport::socket::BusConnection::sendEvent(boost::shared_ptr<rsb::Event>, std::string const&) () from /usr/lib/librsbcore.so.0.7.3
```

```
#4 0x00007ffff786b2ea in rsb::transport::socket::BusServer::handleIncoming(boost::shared_ptr<rsb::Event>, boost::shared_ptr<rsb::transport::socket::BusConnection>) () from /usr/lib/librsbcore.so.0.7.3
```

```
#5 0x00007ffff7856c0b in rsb::transport::socket::BusConnection::handleReadBody(boost::system::error_code const&, unsigned long, unsigned long) () from /usr/lib/librsbcore.so.0.7.3
```

```
#6 0x00007ffff78602b1 in void boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>::call<boost::shared_ptr<rsb::transport::socket::BusConnection>, boost::system::error_code const, unsigned long, unsigned long>(boost::shared_ptr<rsb::transport::socket::BusConnection>&, void const*, boost::system::error_code const&, unsigned long&, unsigned long&) const () from /usr/lib/librsbcore.so.0.7.3
```

```
#7 0x00007ffff785ff08 in void boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>::operator()<boost::shared_ptr<rsb::transport::socket::BusConnection>>(boost::shared_ptr<rsb::transport::socket::BusConnection>&, boost::system::error_code const&, unsigned long, unsigned long) const () from /usr/lib/librsbcore.so.0.7.3
```

```
#8 0x00007ffff785f647 in void boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>>, boost::arg<1> (*), boost::arg<2> (*), boost::_bi::value<unsigned int>>::operator()<boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>, boost::_bi::list2<boost::system::error_code const&, unsigned long const&>>(boost::_bi::type<void>, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>&, boost::_bi::list2<boost::system::error_code const&, unsigned long const&>&, int) () from /usr/lib/librsbcore.so.0.7.3
```

```
#9 0x00007ffff785f194 in void boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>>, boost::arg<1> (*),
```



```
boost::arg<2> (*)(), boost::_bi::value<unsigned int> > >, boost::system::error_code, unsigned long>,
boost::asio::basic_stream_socket<boost::asio::ip::tcp, boost::asio::stream_socket_service<boost::asio::ip::tcp> >,
boost::asio::mutable_buffers_1, boost::asio::detail::transfer_all_t, boost::_bi::bind_t<void, boost::_mfi::mf3<void,
rsb::transport::socket::BusConnection, boost::system::error_code const&, unsigned long, unsigned long>,
boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection> >, boost::arg<1> (*)(),
boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >
>(boost::asio::detail::binder2<boost::asio::detail::read_op<boost::asio::basic_stream_socket<boost::asio::ip::tcp,
boost::asio::stream_socket_service<boost::asio::ip::tcp> >, boost::asio::mutable_buffers_1, boost::asio::detail::transfer_all_t,
boost::asio::detail::transfer_all_t, boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection,
boost::system::error_code const&, unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>
>, boost::arg<1> (*)(), boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >*) () from /usr/lib/librsbcore.so.0.7.3
#15 0x00007ffff7860d03 in void
boost_asio_handler_invoke_helpers::invoke<boost::asio::detail::binder2<boost::asio::detail::read_op<boost::asio::basic_stream_socket<boost::asio::ip::tcp,
boost::asio::stream_socket_service<boost::asio::ip::tcp> >, boost::asio::mutable_buffers_1,
boost::asio::detail::transfer_all_t, boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection,
boost::system::error_code const&, unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>
>, boost::arg<1> (*)(), boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >
>(boost::asio::detail::binder2<boost::asio::detail::read_op<boost::asio::basic_stream_socket<boost::asio::ip::tcp,
boost::asio::stream_socket_service<boost::asio::ip::tcp> >, boost::asio::mutable_buffers_1, boost::asio::detail::transfer_all_t,
boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&,
unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>
>, boost::arg<1> (*)(), boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >, boost::system::error_code, unsigned long>
const&, boost::asio::detail::read_op<boost::asio::basic_stream_socket<boost::asio::ip::tcp,
boost::asio::stream_socket_service<boost::asio::ip::tcp> >, boost::asio::mutable_buffers_1, boost::asio::detail::transfer_all_t,
boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&,
unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>
>, boost::arg<1> (*)(), boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >&) () from /usr/lib/librsbcore.so.0.7.3
#16 0x00007ffff7860a07 in boost::asio::detail::reactive_socket_recv_op<boost::asio::mutable_buffers_1,
boost::asio::detail::read_op<boost::asio::basic_stream_socket<boost::asio::ip::tcp,
boost::asio::stream_socket_service<boost::asio::ip::tcp> >, boost::asio::mutable_buffers_1, boost::asio::detail::transfer_all_t,
boost::_bi::bind_t<void, boost::_mfi::mf3<void, rsb::transport::socket::BusConnection, boost::system::error_code const&,
unsigned long, unsigned long>, boost::_bi::list4<boost::_bi::value<boost::shared_ptr<rsb::transport::socket::BusConnection>
>, boost::arg<1> (*)(), boost::arg<2> (*)(), boost::_bi::value<unsigned int> > > >
>::do_complete(boost::asio::detail::task_io_service*, boost::asio::detail::task_io_service_operation*,
boost::system::error_code, unsigned long) ()
    from /usr/lib/librsbcore.so.0.7.3
#17 0x00007ffff78739a3 in boost::asio::detail::task_io_service::complete(boost::asio::detail::task_io_service&) () from
/usr/lib/librsbcore.so.0.7.3
#18 0x00007ffff78744a3 in
boost::asio::detail::task_io_service::do_one(boost::asio::detail::scoped_lock<boost::asio::detail::posix_mutex&&,

```

```

boost::asio::detail::task_io_service::idle_thread_info* ()
  from /usr/lib/librsbcore.so.0.7.3
#19 0x00007ffff78741bc in boost::asio::detail::task_io_service::run(boost::system::error_code&) () from
/usr/lib/librsbcore.so.0.7.3
#20 0x00007ffff787479f in boost::asio::io_service::run() () from /usr/lib/librsbcore.so.0.7.3
#21 0x00007ffff787ea9e in boost::_mfi::mf0<unsigned long, boost::asio::io_service>::operator()(boost::asio::io_service*) const
() from /usr/lib/librsbcore.so.0.7.3
#22 0x00007ffff787ea0f in unsigned long boost::_bi::list1<boost::_bi::value<boost::asio::io_service*> >::operator()<unsigned
long, boost::_mfi::mf0<unsigned long, boost::asio::io_service>, boost::_bi::list0>(boost::_bi::type<unsigned long>,
boost::_mfi::mf0<unsigned long, boost::asio::io_service>&, boost::_bi::list0&, long) () from /usr/lib/librsbcore.so.0.7.3
#23 0x00007ffff787e9bd in boost::_bi::bind_t<unsigned long, boost::_mfi::mf0<unsigned long, boost::asio::io_service>,
boost::_bi::list1<boost::_bi::value<boost::asio::io_service*> > >::operator()() ()
  from /usr/lib/librsbcore.so.0.7.3
#24 0x00007ffff787e868 in boost::detail::thread_data<boost::_bi::bind_t<unsigned long, boost::_mfi::mf0<unsigned long,
boost::asio::io_service>, boost::_bi::list1<boost::_bi::value<boost::asio::io_service*> > >::run() () from
/usr/lib/librsbcore.so.0.7.3
#25 0x00007ffff6e82ba9 in thread_proxy () from /usr/lib/libboost_thread.so.1.46.1
#26 0x00007ffff6c60efc in start_thread () from /lib/x86_64-linux-gnu/libpthread.so.0
#27 0x00007ffff569159d in clone () from /lib/x86_64-linux-gnu/libc.so.6
#28 0x0000000000000000 in ?? ()

```

(gdb) info threads

Id	Target Id	Frame
17	Thread 0x7ffffde390700 (LWP 19940)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
16	Thread 0x7ffffdeb91700 (LWP 19939)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
15	Thread 0x7ffffdf392700 (LWP 19938)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
14	Thread 0x7ffffdfb93700 (LWP 19937)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
13	Thread 0x7ffffe0394700 (LWP 19936)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
12	Thread 0x7ffffe0b95700 (LWP 19935)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
11	Thread 0x7ffffe1396700 (LWP 19934)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
10	Thread 0x7ffffe1b97700 (LWP 19933)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
9	Thread 0x7ffffe2398700 (LWP 19932)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
8	Thread 0x7ffffe2b99700 (LWP 19931)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
7	Thread 0x7ffffe339a700 (LWP 19930)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
6	Thread 0x7ffffe3b9b700 (LWP 19929)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
5	Thread 0x7ffffe439c700 (LWP 19928)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
4	Thread 0x7ffffe4b9d700 (LWP 19927)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0
3	Thread 0x7ffffe539e700 (LWP 19926)	"rsb_videoreceiv" 0x00007ffff6c6504c in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/x86_64-linux-gnu/libpthread.so.0

/lib/x86_64-linux-gnu/libpthread.so.0

* 2 Thread 0x7fffe5b9f700 (LWP 19925) "rsb_videoreceiv" 0x00007ffff5c0956b in std::string::assign(std::string const&) () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6

1 Thread 0x7ffff7fa5960 (LWP 19922) "rsb_videoreceiv" 0x00007ffff5c20e93 in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6

Related issues:

Copied to Robotics Service Bus - Bug # 1546: Socket server dies because of in...

Resolved

09/20/2012

Associated revisions**Revision 3a5aa0c3 - 10/02/2012 10:42 PM - J. Moringen**

Fixed memory corruption issue in socket transport

refs #1173

- src/rsb/transport/socket/InPullConnector.cpp: when handling an event, copy it prior to any modification
- src/rsb/transport/socket/InPushConnector.cpp: likewise
- test/rsb/transport/socket/SocketServerRoutingTest.cpp: new file; test routing of events by a BusServer with several connectors and connections
- test/rsb/transport/ConnectorTest.cpp: deactivate connectors after use; this is necessary for socket transport connectors
- test/CMakeLists.txt:
test/rsb/transport/socket/SocketServerRoutingTest.cpp

Revision ddac3c64 - 10/04/2012 01:20 PM - J. Moringen

Backport: Fixed memory corruption issue in socket transport

refs #1173

- src/rsb/transport/socket/InPullConnector.cpp: when handling an event, copy it prior to any modification
- src/rsb/transport/socket/InPushConnector.cpp: likewise
- test/rsb/transport/socket/SocketServerRoutingTest.cpp: new file; test routing of events by a BusServer with several connectors and connections
- test/rsb/transport/ConnectorTest.cpp: deactivate connectors after use; this is necessary for socket transport connectors
- test/CMakeLists.txt:
test/rsb/transport/socket/SocketServerRoutingTest.cpp

History**#1 - 09/20/2012 03:43 PM - J. Moringen**

- Assignee deleted (J. Moringen)

I cannot debug this now.

However, I suspect this to be caused by a threading problem: the connection(s) in question seem to be destructed from two threads in parallel:

1. One threads fails to send data and decides to destruct the connection
2. The other thread fails to receive data and decides to destruct the connection

#2 - 09/20/2012 04:06 PM - J. Wienke

This problem only appears if one of the programs on the remote computer is the server for the socket transport. What is also interesting is that in this case sometimes the common lisp logger dies:

```
humavips@HUMAVIPS:~/Downloads$ ~/work/RSB-0.7/bin/logger socket:/nao/vision/0
```

WARNING:

Failed to load Spread library: Unable to load any of the alternatives:

("libspread-without-signal-blocking.so" "libspread.so" "libspread.so.2"

"libspread.so.2.0" "libspread.so.1").

Did you set LD_LIBRARY_PATH?

Spread transport will now be disabled.

The encoded data

```
#<NOTIFICATION {100B07DE73}>
```

could not be decoded :

After unpacking, the notification

```
#<RSB.PROTOCOL:NOTIFICATION {100B07DE73}>
```

[standard-object]

Slots with :INSTANCE allocation:

```
EVENT-ID = #<RSB.PROTOCOL:EVENT-ID {100B07DEE3}>
```

```
SCOPE = #(47 110 97 111 47 118 105 115 105 111 110 47 48 47)
```

```
METHOD = #()
```

```
WIRE-SCHEMA = #(46 114 115 116 46 118 105 115 105 111 110 46 73 109 97 103 101)
```

```
DATA = #(46 114 115 116 46 118 105 115 105 111 110 46 73 109 97 103 101)
```

```
CAUSES = #()
```

```
META-DATA = #<RSB.PROTOCOL:EVENT-META-DATA {100B07E5F3}>
```

could not be converted into an event.

Caused by:

```
> The wire data #(46 114 115 116 46 118 105 115 105 111 110 46 73 109 97 103 101) (in :|.rst.vision.Image| wire-schema) could not be converted to domain type :UNDETERMINED
```

```
> Caused by:
```

```
>> Invalid wire-type designator 6 at offset 0 (no such wire-type).
```

In the case where the robot itself provides the server everything is ok, but the performance is unacceptable in this topology as the robot needs to route every message with its limited CPU.

#3 - 09/20/2012 04:07 PM - J. Wienke

Jan Moringen wrote:

However, I suspect this to be caused by a threading problem: the connection(s) in question seem to be destructed from two threads in parallel:

1. *One threads fails to send data and decides to destruct the connection*

Why actually could it fail to send data?

1. *The other thread fails to receive data and decides to destruct the connection*

#4 - 09/20/2012 04:22 PM - J. Moringen

Johannes Wienke wrote:

| *Why actually could it fail to send data?*

Because the remote end already closed the socket.

#5 - 09/20/2012 04:23 PM - J. Moringen

The problem should be fixed in the trunk version of the logger.

You can try the following - Use a CL logger as server (maybe with --style discard)

- Use something like --on-error recover or similar

This should work in the 0.7 version of the logger.

#6 - 09/20/2012 04:25 PM - J. Wienke

Actually in that case the logger wasn't the server.

Can you backport the fixes to 0.7. It is really important that 0.7 is maintained well now.

#7 - 09/20/2012 04:53 PM - J. Wienke

So, just as summary: We are unable to receive images from NAO on a remote computer reliably using the socket transport. It always crashes with the backtrace found above, on different computers. Other data types however worked. So I could imagine it is related to the data size or the huge bandwidth created by 2*20 Hz VGA YUV422 images. The program we tried for receiving (RsbVideoReceiver) works perfectly with the spread transport.

If we do not find an immediate solution to this problem we should provide RSB debian packages with spread included.

#8 - 10/02/2012 07:32 PM - J. Moringen

- *Status changed from New to In Progress*
- *Assignee set to J. Moringen*

#9 - 10/08/2012 04:05 PM - J. Wienke

- *Status changed from In Progress to New*
- *Assignee deleted (J. Moringen)*

I think we could resolve this now? And we should also add a copy to 0.8

#10 - 10/08/2012 04:06 PM - J. Wienke

- Status changed from *New* to *In Progress*
- Assignee set to *J. Moringen*

Why did redmine delete the association etc?

#11 - 10/10/2012 12:52 PM - J. Wienke

Jan?

#12 - 10/10/2012 01:03 PM - J. Moringen

We can probably close this issue, although we may not yet have fixed everything.

I am still not sure about the initial symptom before the segmentation fault:

```
humavips@HUMAVIPS:~/work$ ~/work/RSB-0.7/bin/rsb_videoreceiver
1348146353274 rsb.transport.socket.BusServer [WARN]: Send failure (Connection reset by peer); will close connection later
1348146353276 rsb.transport.socket.BusServer [WARN]: Send failure (Connection reset by peer); will close connection later
1348146353280 rsb.transport.socket.BusConnection [WARN]: Receive failure (error asio.misc:2) or incomplete message body (received 25341
bytes); closing connection
1348146353291 rsb.transport.socket.BusConnection [WARN]: Receive failure (error asio.misc:2) or incomplete message body (received 510
bytes); closing connection
Segmentation fault
```

But with our fixes applied, it should be much easier to diagnose that problem, if there is one. We can create a new issue, if this is still not completely fixed.

Not sure, whether we should a copy of the issue to version:rsb-0.8.

#13 - 10/10/2012 01:04 PM - J. Wienke

It is fixed in 0.8, too. So would be nice if it was recorded in the issue tracker.

#14 - 06/21/2013 08:50 AM - J. Wienke

- Status changed from *In Progress* to *Resolved*

From the comments I suspect this is resolved and I did not see such a crash again.