In-Lab

To analyze an RLC-layer PCAP using Wireshark, you will need to configure User DLT 149 for UDP and enable the rlc_nr_udp protocol:

1. Go to Edit->Preferences->Protocols->DLT_USER->Edit and add an entry with DLT=149 and Payload protocol=udp.
2. Go to Analyze->Enabled Protocols->RLC-NR and enable rlc_nr_udp
3. Go to Edit->Preferences->Protocols->RLC-NR and configure according to your needs.

RLC: Overview / Overall Functionality

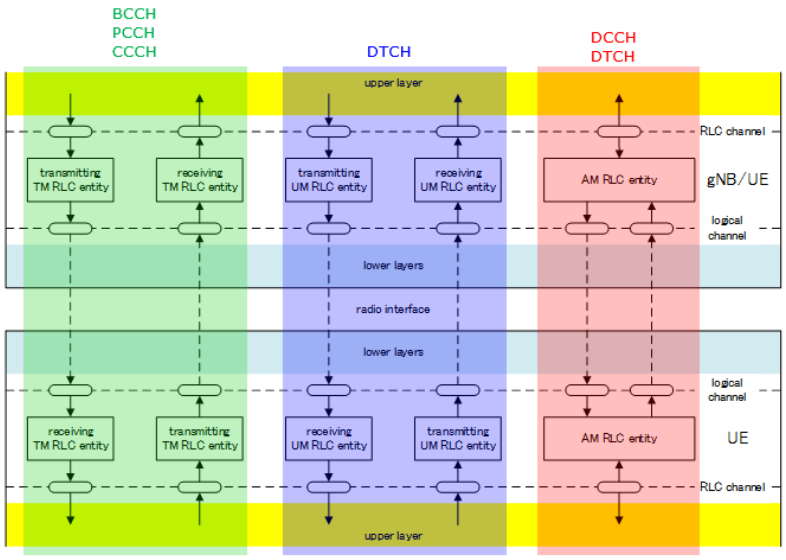
NR RLC has three different mode: TM(Transparent Mode), UM(Unacknowledge Mode) and AM(Acknowledge mode). The very brief summary of key features of these mode is as follows :

1. TM : No RLC Header, Buffering at Tx only, No Segmentation/Reassembly, No feedback (i.e, No ACK/NACK)
2. UM : RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, No feedback(i.e, No ACK/NACK)
3. AM : RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, Feedback(i.e, ACK/NACK)

Each of these modes can both transmit and receive data. In TM and UM, separate entity is used for transmission and reception, but in AM a single RLC entity perform both transmission and reception as illustrated below.

Each of logical channels use a specific RLC mode as shown below.

- BCCH, PCCH, CCCH use RLC TM only.
- DCCH use RLC AM only.
- DTCH use RLC UM or AM. (Which mode is used for each DTCH channel? This is determined by RRC message).



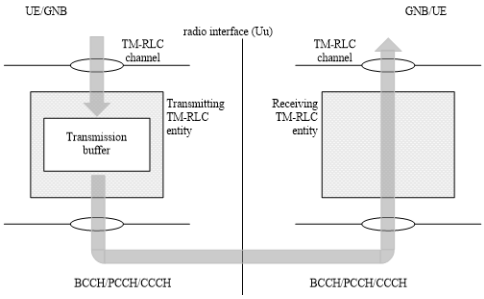
RLC mode and logical channels

TM Mode / Procedure

As you see in the following illustration. TM mode would mean ‘almost no processing to RLC data’. The only thing it does is to buffer data on Tx side. There is no RLC header, No reordering, no segmentation, no reassembly is happening in this layer. Because of this ‘no data processing’ nature of TM mode, if you compare the RLC input and RLC output data of TM mode, you would see no difference between the two.

One important thing to keep in mind is that you need to pay attention to MAC/PHY resource allocation. Even if MAC/PHY resource is allocated smaller than the RLC packet, the RLC wouldn’t care. It would just forward whatever it has to MAC/PHY. So those RLC data bigger than MAC/PHY resource may be chopped off or discarded.

Again another this to be noticed is that the local channel BCCH/PCCH/CCCH data is processed by this RLC mode.



Model of two transparent mode peer entities

UM Mode / Procedure

Next, let’s look into UM mode. UM stands for ‘Unacknowledged Mode’. ‘Unacknowledged Mode’ means ‘it does not require any reception response from the other party’. ‘Reception response’ simply mean ‘ACK’ or ‘NACK’ from the other party. (UM mode is similar to TM mode in that it does not require any ACK/NACK from the other party, but it is different from TM in that I has it’s own header)

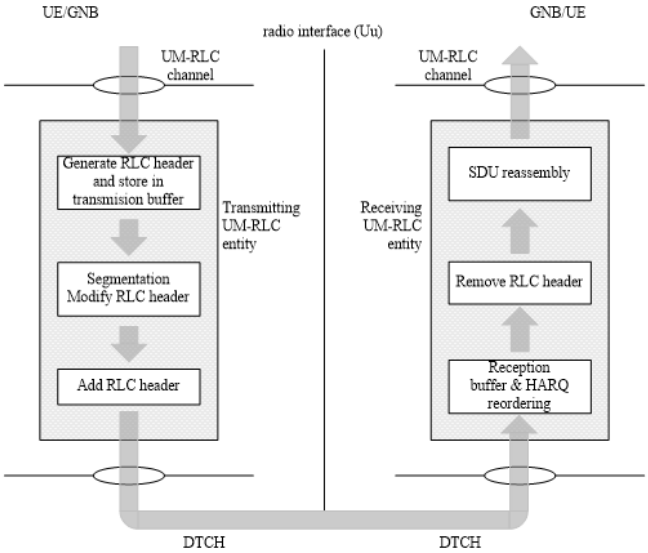
Let’s read the operation on transmitting side.

- Buffering the data and generate RLC Header.
- Segmentation (Split a big chunk into a multiple small chunk) and Modify RLC Header (Some field in RLC header should be changed based on the segmentation status)
- Add RLC header

Then, read the operation on receiving side.

- Buffering

- Reordering (Sometimes the chunks transmitted earlier from transmitter may arrive late at the receiver. In this case you have to reorder the incoming chunks into proper order for reassembly).
- Remove the RLC header (you would remember that the transmitter put the header to each of the chunk. So, you have to remove this before you reassemble the data).
- Reassembly



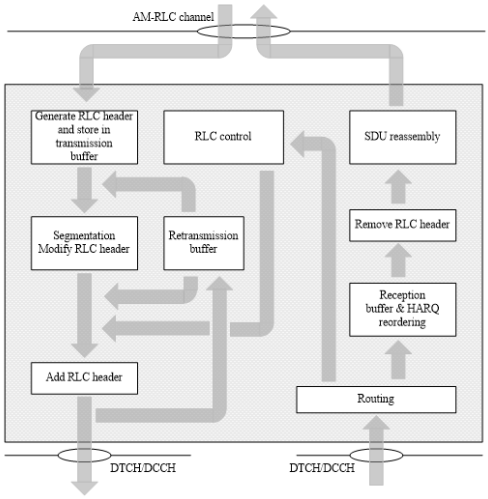
Model of two unacknowledged mode peer entities

AM Mode / Procedure

Now let's look at AM mode which is the most complicated RLC type. 'AM' stands for 'Acknowledge Mode'. As its name implies it requires ACK/NACK from the other party. It is more like TCP packet in IP world, whereas RLC UM is more like UDP in IP world.

After RLC transmitter do the segmentation/concatenation process, it adds RLC header and then it creates two identical copies and transmit the one copy of the data out to lower layer (MAC) and send another copy to Retransmission buffer.

If the RLC get Nack or does not get any response from the other party for a certain period of time, the RLC packet (we call this RLC PDU) in the retransmission buffer gets transmitted again. If the RLC get ACK, the ones in retransmission buffer would be discarded.



Model of an acknowledged mode entity

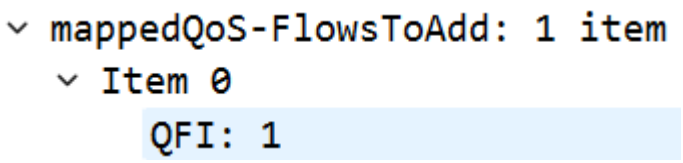
Step 1: Identify the messages with AM, UM, TM modes

protocol	INFORMATION	MODE
NR RRC	RRC Setup Request	TM
NR RRC	RRC Setup	TM
NR RRC/NAS-5GS	RRC Setup Complete, Registration request [102-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer, Identity request [13-bytes]	AM
NR RRC/NAS-5GS	UL Information Transfer, Identity response [34-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer, Authentication request [51-bytes]	AM
NR RRC/NAS-5GS	UL Information Transfer, Authentication response [37-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer, Security mode command [30-bytes]	AM
NR RRC/NAS-5GS	UL Information Transfer [90-bytes]	AM
NR RRC	Security Mode Command [9-bytes]	AM
NR RRC	Security Mode Complete [8-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer [55-bytes]	AM
NR RRC/NAS-5GS	UL Information Transfer [19-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer [60-bytes]	AM
NR RRC	RRC Release [8-bytes]	AM
NR RRC	RRC Setup Request	TM
NR RRC	RRC Setup	TM
NR RRC/NAS-5GS	RRC Setup Complete, Service request [51-bytes]	AM
NR RRC	Security Mode Command	AM
NR RRC	Security Mode Complete [8-bytes]	AM
NR RRC/NAS-5GS	DL Information Transfer [23-bytes]	AM
NR RRC/NAS-5GS	UL Information Transfer [99-bytes]	AM
NR RRC	UE Capability Enquiry [14-bytes]	AM
NR RRC	UE Capability Information	AM
NR RRC/NAS-5GS	RRC Reconfiguration [163-bytes]	AM
NR RRC	RRC Reconfiguration Complete [8-bytes]	AM

DRBs are radio bearers specifically used for carrying user data. This is the actual content that users send and receive, such as internet traffic, video streams, and file downloads. DRBs are closely associated with QoS.

Step 2: In the pcap file identify the network slicing (QoS Flow, QFI), where it was recorded and its messages.

NR RRC/NAS-5GS	RRC Reconfiguration [163-bytes]



SRBs are radio bearers specifically designed to carry signalling information between the User Equipment (UE, or your device) and the network.

SRBs handle the transmission of Radio Resource Control (RRC) messages. These messages are used for tasks like:

- Establishing and releasing connections.
- Configuring radio resources.
- Managing mobility (handovers).
- Handling security procedures.

There are different types of SRBs, each with specific roles:

- **SRB0:** Used for initial access and some basic RRC messages.
- **SRB1:** Used for RRC messages and NAS messages before SRB2 is established.
- **SRB2:** Used for NAS messages after security activation.
- **SRB3:** Used for specific RRC messages in EN-DC (E-UTRA New Radio Dual Connectivity).

Step 3: From the pcap file identify the Signaling Radio Bearer messages