



KAPITEL 5 / CHAPTER 5⁵ FEATURES OF THE RRC RADIO RESOURCE MANAGEMENT PROTOCOL IN THE 5G NETWORK

DOI: 10.30890/2709-2313.2023-20-02-012

Вступ

Протокол рівня управління L3 – це протокол управління радіоресурсами RRC (Radio Resource Control). Об'єкт протоколу RRC як на боці терміналу користувача UE, так і на боці базової мережі оператора має інтерфейси управління з усіма іншими об'єктами протоколу. Щоразу, коли протокольний об'єкт, яким має керувати RRC, перебуває у іншому елементі базової мережі, необхідно підтримувати цей механізм управління з допомогою стандартизованих протоколів. У всіх інших випадках інтерфейси управління є внутрішніми по відношенню до одного елемента UE або базової мережі і, отже, не є стандартизованими, але їх наявність має вирішальне значення для рівня RRC для виконання свого завдання як виконавця рішень з управління радіоресурсами.

5.1. Стек протоколів площини управління (5G control plane)

Протокол управління радіоресурсами RRC (Radio Resource Control) є протоколом площини управління (control plane) і являє собою систему алгоритмів і команд, що використовуються для надання терміналу користувача UE доступу до радіоінтерфейсу і реалізації стратегії управління радіоресурсами мережі 5G-NR. Розташування RRC у стеку протоколів показано на рис. 1.

Нижче наведено основні функції, реалізацію яких забезпечує RRC:

- трансляція системної інформації AS (Access Stratum - рівень сигналізації, що відноситься до середовища доступу та існуючий на ділянці між UE та gNB) / NAS (Non Access Stratum - рівень сигналізації, що не відноситься до середовища доступу та існуючий на ділянці між UE та AMF);

- передача повідомлень пошуку терміналів (пейджинг), ініційованих 5GC і NG-RAN;
- встановлення, підтримка та розрив з'єднання за протоколом RRC між UE та NG-RAN;

⁵Authors: Vetoshko I., Kravchuk S.

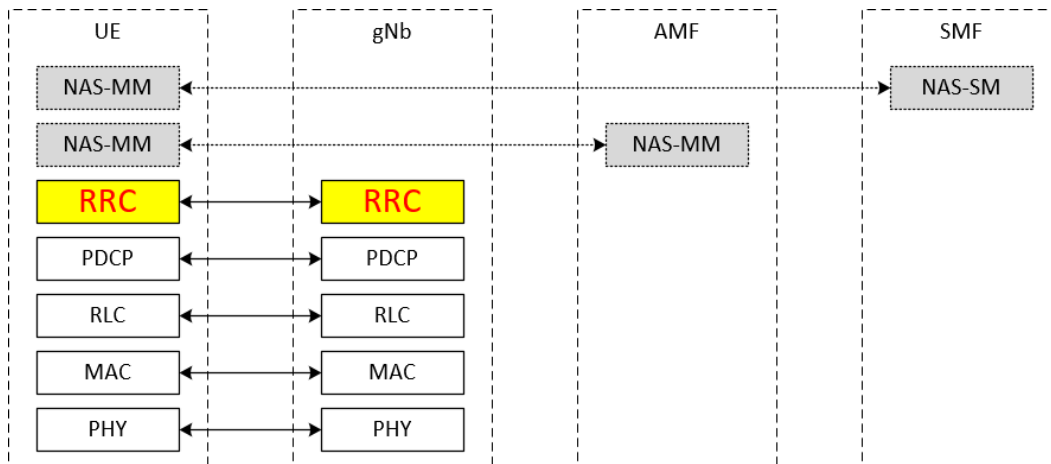


Рисунок 1 - Розташування RRC у стеку протоколів

- управління агрегацією несучих частот (у межах концепції carrier aggregation);
- управління режимом подвійного підключення (Dual Connectivity) – одночасного підключення UE до двох базових станцій (двох gNB, або gNb та ng- eNB);
- виконання завдань безпеки, у тому числі управління ключами шифрування та контролю цілісності даних на радіоінтерфейсі;
- управління віртуальними радіоканалами сигналізації SRB (Signaling Radio Bearers) та передачі даних DRB (Data Radio Bearer);
- управління мобільністю (передача обслуговування (ПОБ), параметрами вибору стільника та технології радіодоступу);
- управління параметрами якості QoS;
- управління UE у частині радіовимірювань та звітності;
- виявлення втрати та відновлення радіоканалу;
- транзитна передача повідомлень NAS сигналізації між UE та модулем управління доступом та мобільністю AMF;
 - підтримка само-конфігурації та само-оптимізації мережі.

5.2. Стани RRC-з'єднань

RRC-з'єднання, створюване між мережею 5G і користувальницьким терміналом UE являє собою кінцевий автомат з трьома можливими станами:



- RRC_IDLE (не підключено),
- RRC_CONNECTED (підключено та активно),
- RRC_INACTIVE (підключено та неактивно).

Таким чином, у мережах 5G-NR визначено новий стан RRC_INACTIVE, який відсутній у мережах попереднього покоління (4G-LTE), і що дозволяє зменшити затримки активації протоколу RRC.

Різні стани RRC з одного боку характеризуються різними радіоресурсами, доступними терміналу для використання, з іншого - різним рівнем інформації про UE, доступну мережу зв'язку. При включенні електроживлення термінал користувача UE виявляється в режимі RRC_IDLE. Підключення до мережі та перехід у стан RRC_CONNECTED здійснюється в рамках процедури початкової реєстрації (Initial Attach). За відсутності активності з боку UE протягом певного часу (визначеного значенням user-inactivity-timer) з'єднання переходить у стан RRC_INACTIVE. Повернення у стан RRC_CONNECTED виконується в рамках процедури відновлення RRC-з'єднання. Перехід у стан RRC_IDLE можливий як з RRC_CONNECTED, так і з RRC_INACTIVE при розриві з'єднання з мережею (Detach), або втрати зв'язку (Connection failure).

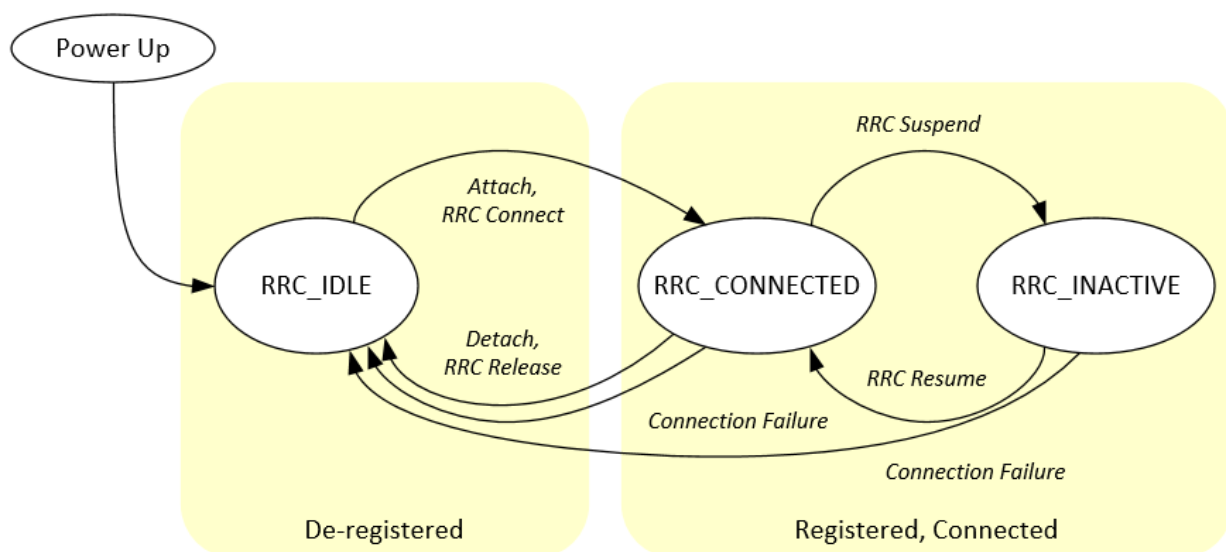


Рисунок 2 - Машина станів RRC-з'єднань

При переході в стан RRC_INACTIVE і UE, і NG-RAN зберігають налаштування радіозв'язку та безпеки. Цей збережений контекст неактивного рівня доступу (AS) UE може швидко відновитися з мінімальною сигналізацією при переході в стан підключення. По суті, RRC_INACTIVE - це спосіб RRC UE реалізувати "завжди активне" радіоз'єднання з мережею.



Машина станів RRC з'єднань наведена на рис. 2.

Таблиця 1 - Термінал користувача UE в різних станах

| UE | Виключення | Attaching (Приєднання) | Підключено/ Неактивно | Підключено/ Активно |
|---------------------------|-----------------|---------------------------|--------------------------------|------------------------|
| Управління реєстрацією | RM-DEREGISTERED | | RM-DEREGISTERED | |
| Управління з'єднанням | CM-IDLE | CM-CONNECTED | | |
| Стан RRC | RRC-IDLE | RRC- CONNECTED | RRC-INACTIVE | RRC- CONNECTED |
| Управління мобільністю | - | на базі UE | на базі UE / з допомогою NW | на базі NW |

У стані *RRC_IDLE* термінал користувача UE (табл. 1):

- здійснює вибір мережі мобільного зв'язку PLMN;
- здійснює вибір/перевибір стільника;
- здійснює прийом широкомовної системної інформації про стільник (MIB, SIB);
- здійснює прийом повідомлень пейджингу, ініційованих опорною мережею 5GC;
- здійснює підтримку режиму уривчастого прийому DRX (Discontinuous Reception) повідомлень пейджингу;
- здійснює оновлення реєстрації RAU (Registration Area Update) за таймером або переміщення в іншу зону реєстрації RA (Registration Area). Розташування UE відоме з точністю до зони реєстрації (RA).

У стані *RRC_INACTIVE* термінал користувача UE:

- здійснює вибір мережі мобільного зв'язку PLMN;
- здійснює вибір/перевибір стільника;
- здійснює прийом широкомовної системної інформації про стільник;
- здійснює прийом повідомлень пейджингу, ініційованих опорною мережею 5GC;
- здійснює підтримку режиму уривчастого прийому DRX (Discontinuous Reception) повідомлень пейджингу;
- здійснює оповіщення мережі радіодоступу NG-RAN про поточне місцезнаходження за таймером або при виході із зони нотифікації RNA (RAN-based Notification Area);
- має встановлене з'єднання з опорною мережею 5GC і мережею



радіодоступу NG-RAN для передачі даних площини управління (control plane) та площини даних користувача (user plane);

- має збережені дані асоціації (контексти) протоколів рівня AS (RRC/PDCP/RLC/MAC).

Розташування UE відоме з точністю до зони нотифікації RNA, яка значно менше зони реєстрації RA і включає одну або кілька стільників.

У стані *RRC_CONNECTED* користувальницький термінал UE:

- має встановлене з'єднання з опорною мережею 5GC і мережею радіодоступу NG-RAN для передачі даних площини управління та площини даних користувача;

- перебуває в активному стані та здійснює прийом/передачу даних;

- при переміщенні в інший стільник виконує ПОб;

- має збережені дані асоціації (контексти) протоколів рівня AS (RRC/PDCP/RLC/MAC);

- виконує вимірювання параметрів мережі радіодоступу відповідно до отриманих вказівок.

Розташування UE відоме з точністю до стільника. Управління мобільністю UE (включаючи зміну технології доступу) здійснюється мережею, зокрема, на підставі одержаних від терміналу звітів з результатами вимірювань. Відповідно до можливостей терміналу та мережі зв'язку можуть бути використані технології агрегації частот та подвійного підключення.

Повідомлення протоколу управління радіоресурсами RRC передаються по віртуальних радіоканалах сигналізації SRB:

- SRB0 - для передачі повідомлень RRC за загальним логічним каналом CCCH;

- SRB1 – для передачі RRC, а також NAS повідомлень до встановлення SRB2; використовується виділений логічний канал DCCH;

- SRB2 (встановлюється після активації механізмів безпеки) – для передачі NAS повідомлень; використовується виділений логічний канал DCCH;

- SRB3 - для передачі RRC повідомлень у режимі подвійного підключення до мережі 5G-RAN та E-UTRA.



5.3. Основні процедури, що реалізуються RRC

Доставка користувачьким терміналам системної інформації (NR-MIB, NR-SIB). Системна інформація, що передається базовими станціями 5G-NR, містить різні конфігураційні параметри радіоінтерфейсу, необхідні користувальницьким терміналам UE для здійснення доступу до мережі, прийому та передачі даних. Системна інформація передається в MIB (Master Information Block) та SIB (System Information Block) блоках. MIB-блок передається фізичним каналом PBCH, SIB-блоки – PDSCH. У мережах 4G-LTE всі блоки системної інформації передаються з певним періодом у широкомовному режимі і приймаються всіма UE, що знаходяться в зоні дії відповідних стільників мережі. 5G-NR блоки MIB і SIB1 передаються в широкомовному режимі; інші SIB-блоки (залежно від політики оператора зв'язку) можуть передаватися або також у широкомовному режимі, або у виділених каналах на запит конкретних UE (рис. 3). Інформація про те, які блоки передаються на запит, а які в широкомовному режимі та параметри їх передачі міститься в SIB1.

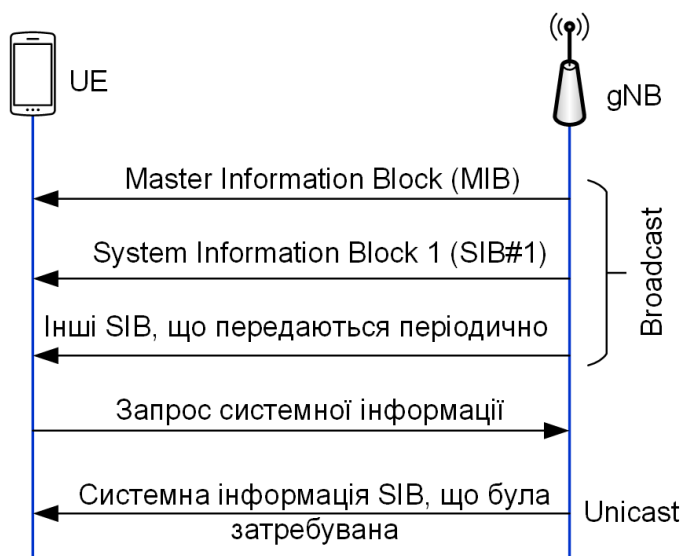


Рисунок 3 - Передача системної інформації

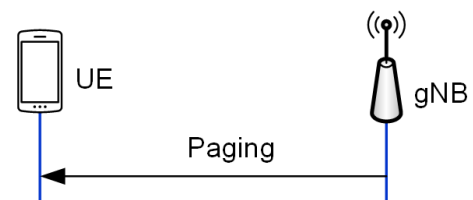


Рисунок 4 - Процедура пейджингу

Пейджинг (Paging). Процедура пейджингу використовується для пошуку терміналу користувача, що знаходиться в станах RRC-IDLE / RRC_INACTIVE, з метою встановлення з ним вхідного з'єднання (рис. 4).

Управління з'єднанням (Connection control). Включає в себе:

- створення RRC-з'єднання, зокрема, організацію віртуального радіоканалу сигналізації SRB1 (SRB1-повідомлення передаються без шифрування та контролю цілісності) (рис. 5, а);

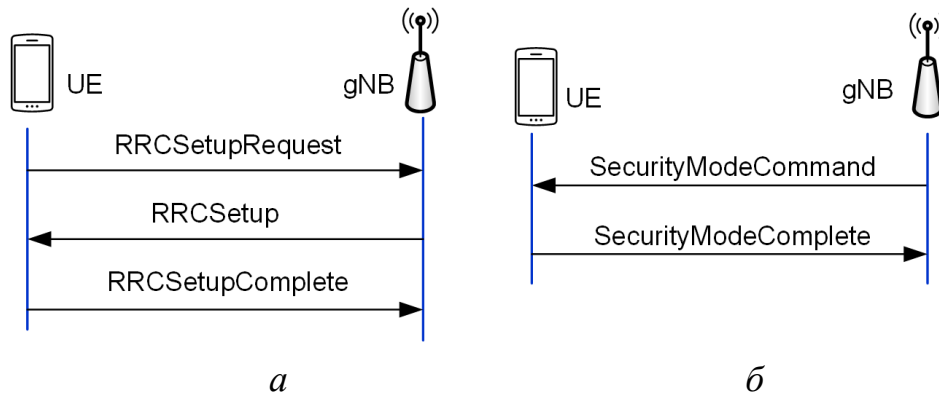


Рисунок 5 - Створення RRC-з'єднання (а) та активація механізмів безпеки (б)

- активацію механізмів безпеки на радіоінтерфейсі (шифрування та контроль цілісності повідомлень сигнального та користувацького трафіку) - після отримання від 5GC контексту терміналу користувача (UE-context); при цьому і запит (SecurityModeCommand) та відгук (SecurityModeComplete) передаються з контролем цілісності, але у відкритому (нешифрованому) вигляді; всі наступні повідомлення в рамках організованого RRC-з'єднання передаються у закритому вигляді (рис. 5, б);

- реконфігурацію RRC з'єднання та організацію віртуального каналу сигналізації SRB2 (SRB3) і віртуального каналу трафіку користувача DRB (рис. 6, а);

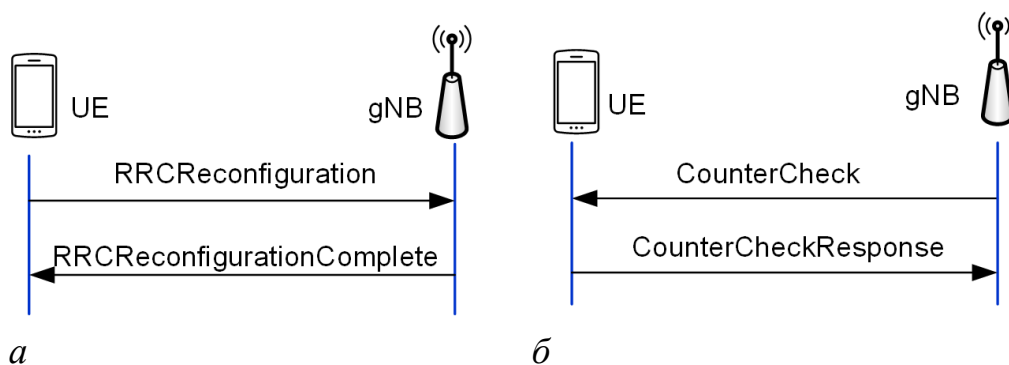


Рисунок 6 - Реконфігурація RRC з'єднання (а) та звірення обсягів переданого та прийнятого трафіку (б)

- звірення обсягів переданого та прийнятого трафіку, що дозволяє, зокрема,

виявити "вставку" хибних пакетів з боку зломисників (атаки типу "людина посередині") (рис. 6, б);

- повторне встановлення RRC-з'єднання (наприклад, у разі втрати мережі користувачьким терміналом); у разі відсутності на мережі дійсного UE-контексту, ця процедура ініціює виконання процедури створення RRC-з'єднання (рис. 7);

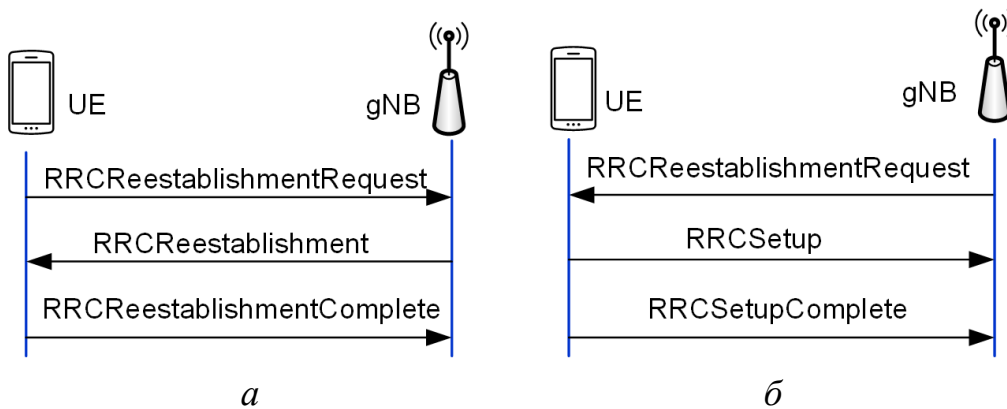


Рисунок 7 - Повторне встановлення RRC-з'єднання: а – на мережі має місце дійсний UE-контекст; б – на мережі відсутній дійсний (валідний) UE-контекст – повернення до процедури створення RRC-з'єднання

- ініційований мережею розрив RRC-з'єднання; ця процедура може бути використана в т.ч. для перекладу терміналу користувача в іншу мережу радіодоступу (E-UTRAN) (рис. 8);

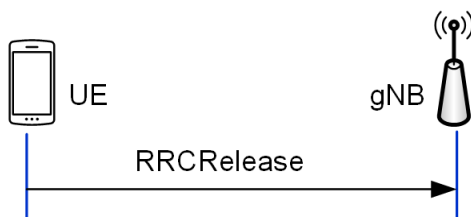


Рисунок 8 - Ініційований мережею розрив RRC-з'єднання

- ініційована мережею припинення RRC з'єднання та переведення RRC у стан RRC_INACTIVE;

- розрив RRC з'єднання з ініціативи верхнього рівня терміналу користувача (upper-layer UE) (рис. 9);

- виявлення та відновлення втрати зв'язку (Radio link failure).

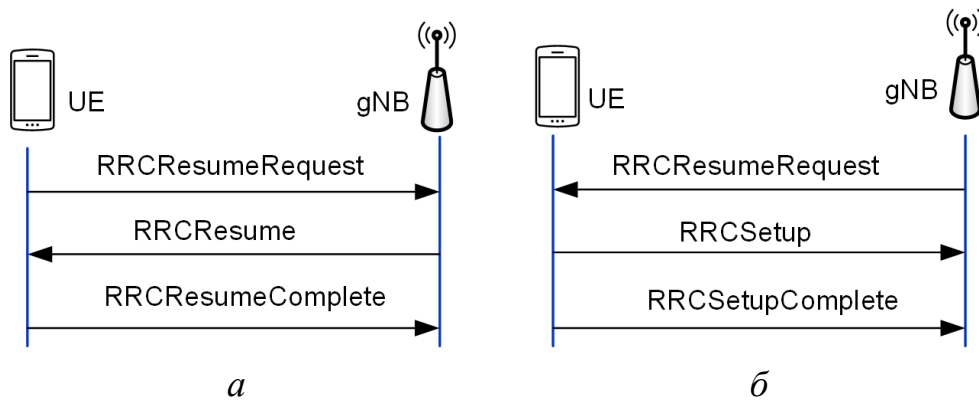


Рисунок 9 - Розрив RRC з'єднання з ініціативи верхнього рівня терміналу:
а – на мережі має місце дійсний UE-контекст; ***б*** – на мережі відсутній дійсний (валідний) UE-контекст – повернення до процедури створення RRC-з'єднання

Зміна мережі радіодоступу (вхідна/вихідна ПОб між NR та E-UTRA) (рис. 10).

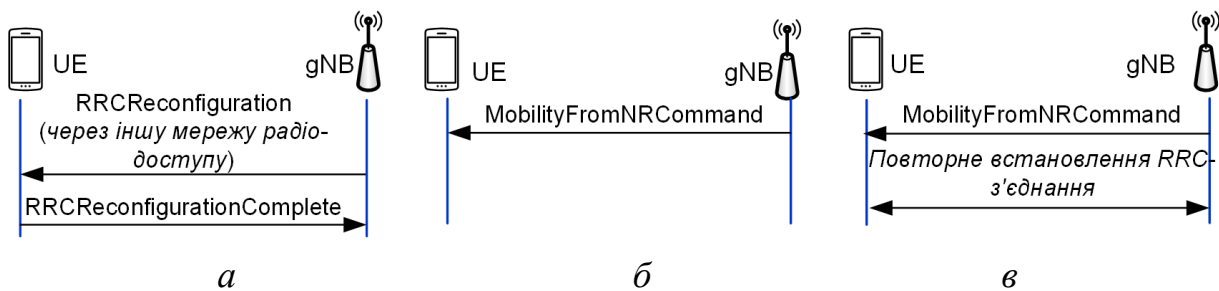


Рисунок 10 - Процедури ПОб: *а* – ПОб в мережу 5G-NR; ***б*** -вдала ПОб із мережі 5G-NR; ***в*** – невдала ПОб із мережі 5G-NR

Запит можливостей терміналу користувача (UE capability) (рис. 11).

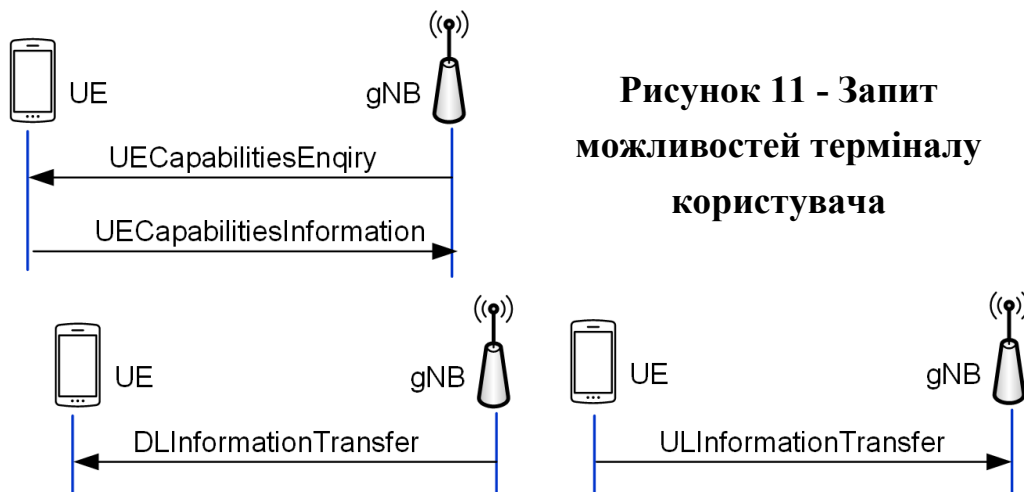


Рисунок 11 - Запит можливостей терміналу користувача

Рисунок 12 - Надсилання повідомлення сигнального трафіку NAS



Надсилання повідомлення сигнального трафіку NAS (DL information transfer, UL information transfer) (рис. 12).

Конфігурація радіовимірювань (включаючи вимірювання на мережі NR та E-UTRA).

Висновки

Представлені можливості розширення функціоналу мережі мобільного оператора 5-го покоління шляхом застосування нових функцій протоколу рівня RRC. Розглянуто стек протоколів площини управління (5G control plane), стани RRC-з'єднань та основні процедури, що реалізуються RRC.