

Лекция №4. Нумерация и идентификация в сети 5G, основы безопасности

1. Виды нумерации и идентификации абонентского терминала в сети мобильной связи

2. Нумерация и идентификация абонентского терминала, используемая в опорной сети 5GC

- международный идентификатор подписки абонента на сервисы сети 5G (SUPI)
- закрытый международный постоянный идентификатор подписки абонента на сервисы сети 5G (SUCI)
- уникальный идентификатор абонентского оборудования (PEI)
- глобальный временный уникальный идентификатор абонента (5G-GUTI)
- глобальный идентификатор сетевой AMF (GUAMI)
- временный идентификатор мобильного абонента сети 5G (5G-TMSI)

3. Нумерация и идентификация абонентского терминала в подсистеме IMS

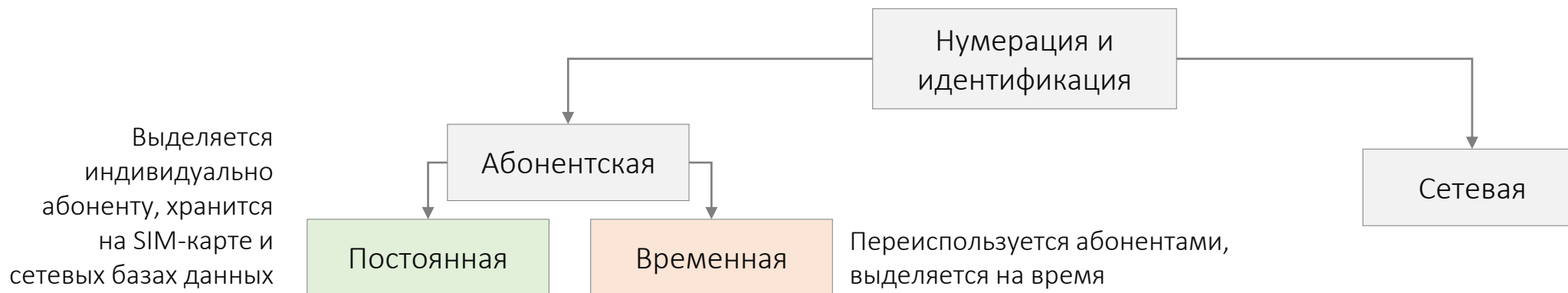
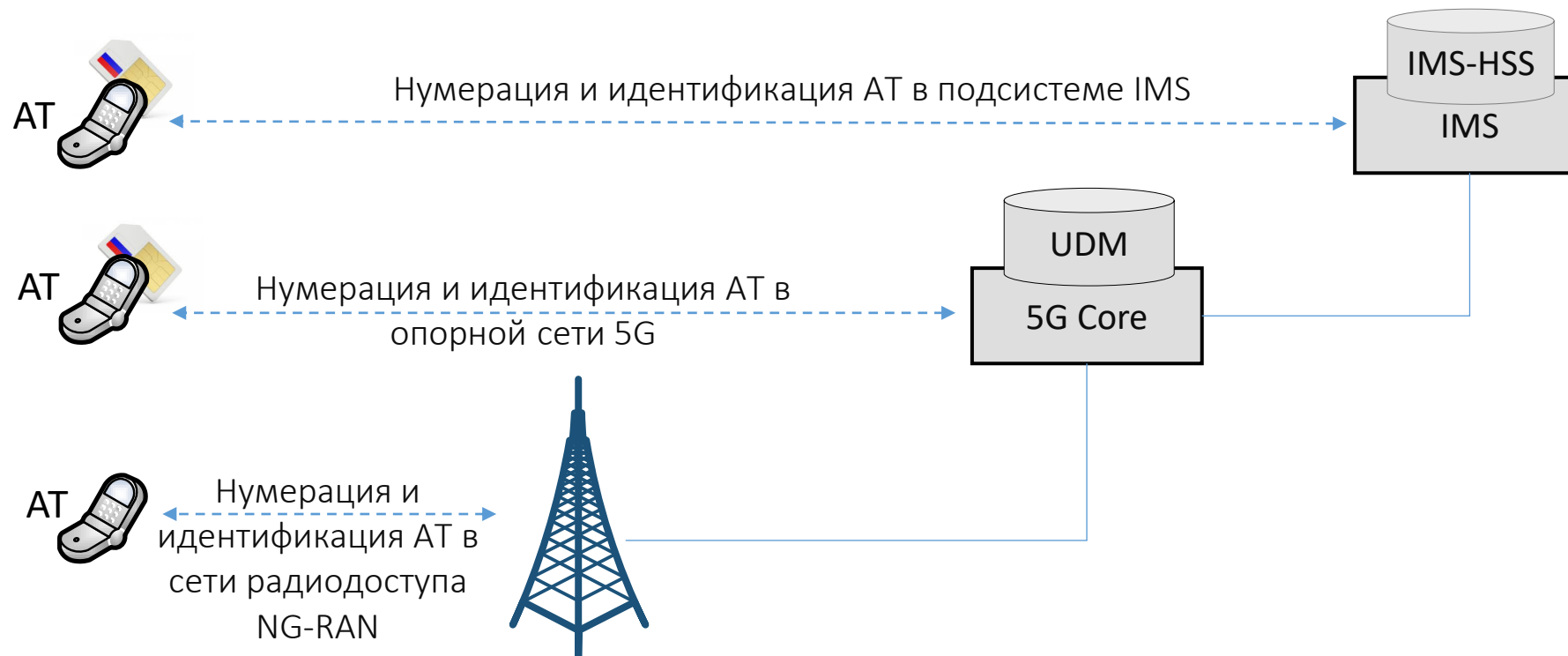
4. Идентификация, используемая в сети радиодоступа NG-RAN

- международный идентификатор базовой станции (Global gNB ID)
- международный идентификатор зоны местоположения абонента (5GS TAI)
- международный идентификатор соты (NCGI)
- код зоны нотификации абонента (RNAC)
- временные идентификаторы абонентского терминала (RNTI)

5. Идентификация, используемая в опорной сети 5GC

- доменные имена сетевых функций
- сетевые слои (Slices)
- IP-адресация

1. Виды нумерации и идентификации абонентского терминала в сети мобильной связи

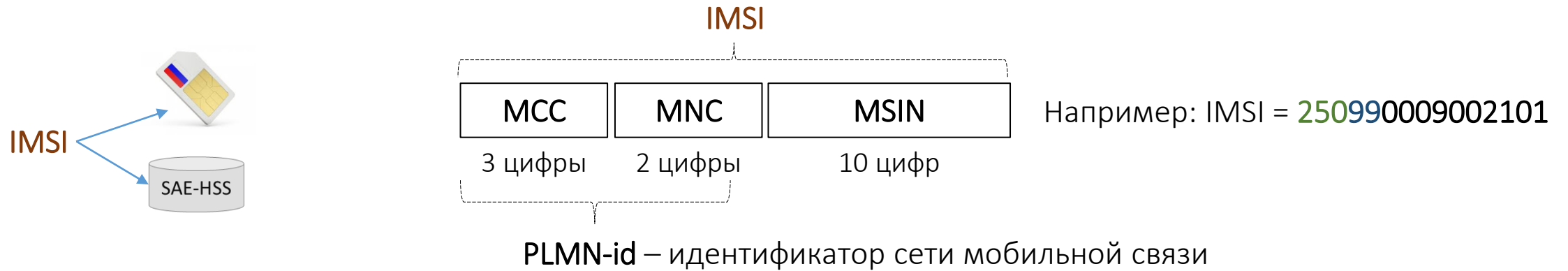


2. Нумерация и идентификация абонентского терминала в опорной сети 5GC

Идентификация/ нумерация	Пояснение	Формат представления	
		1	2
SUPI (Subscription Permanent Identifier)	Международный постоянный идентификатор подписки абонента на сервисы сети 5G	IMSI (тип 0)	NAI (тип 1) Network Access Identifier = username@realm: imsi@nai.5gc.mnc02.mcc250.3gppnetwork.org
SUCI (Subscription Concealed Identifier)	Закрытый международный постоянный идентификатор подписки абонента на сервисы сети 5G	Зашифрованный идентификатор SUPI. Формат идентификатора SUCI определяется форматом идентификатора SUPI.	
PEI (Permanent Equipment Identifier)	Уникальный идентификатор абонентского оборудования	IMEI	IMEISV
5G-GUTI (5G Globally Unique Temporary Identifier)	Глобальный временный уникальный идентификатор абонента. Используется вместо SUCI на временной основе	<5G-GUTI>:= <GUAMI> <5G-TMSI>	
GUAMI (Globally Unique AMF Identifier)	Глобальный идентификатор сетевой функции управления доступом и мобильностью AMF, которая назначила абоненту временный идентификатор 5G-GUTI		
5G-TMSI (5G Temporary Mobile Subscription Identifier)	Временный идентификатор мобильного абонента сети 5G	Двоичное число (32 бита)	

2. Нумерация и идентификация абонентского терминала в опорной сети 5GC

1. Уникальный международный идентификатор абонента сети мобильной связи **IMSI (International Mobile Subscriber Identity)** – постоянный идентификатор, хранится в базе данных SAE-HSS, USIM-карте



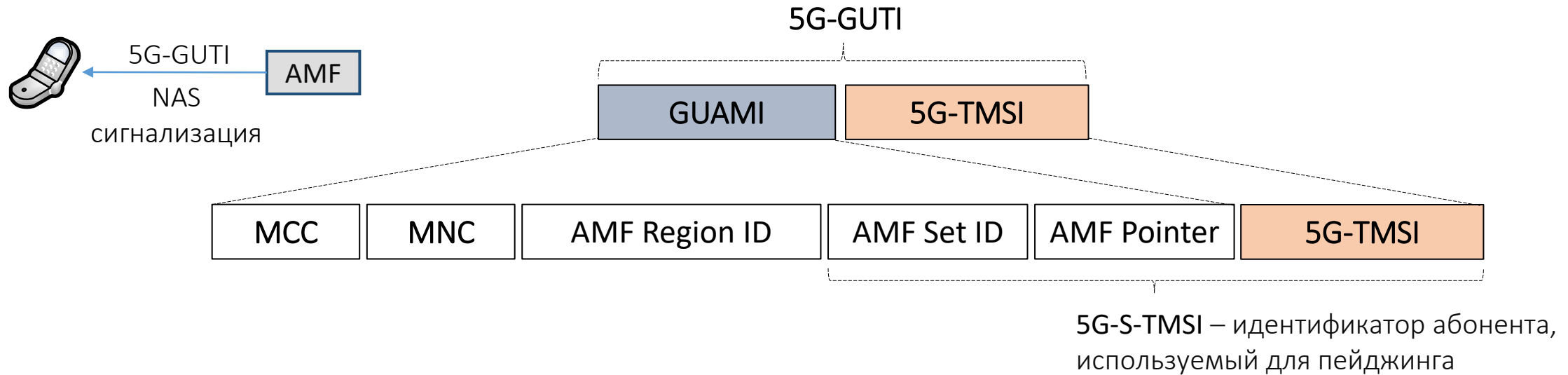
MCC (Mobile Country Code) – код страны, которой принадлежит сеть мобильной связи
MCC = 250 (Российская Федерация)

MNC (Mobile Network Code) – код сети мобильной связи
MNC = 01 (МТС)
MNC = 02 (МегаФон)
MNC = 99 (Билайн)

MSIN (Mobile Subscriber Identification Number) – идентификационный номер абонента сети мобильной связи
MSIN = 0 – 9 999 999 999 (10 млрд. абонентов на один код PLMN-id)

2. Нумерация и идентификация абонентского терминала в опорной сети 5GC

2. Уникальный временный международный идентификатор абонента сети мобильной связи 5G-GUTI (5G Globally Unique Temporary Identifier)



GUAMI (Globally Unique Identifier) – глобальный идентификатор модуля управления доступом и мобильностью AMF

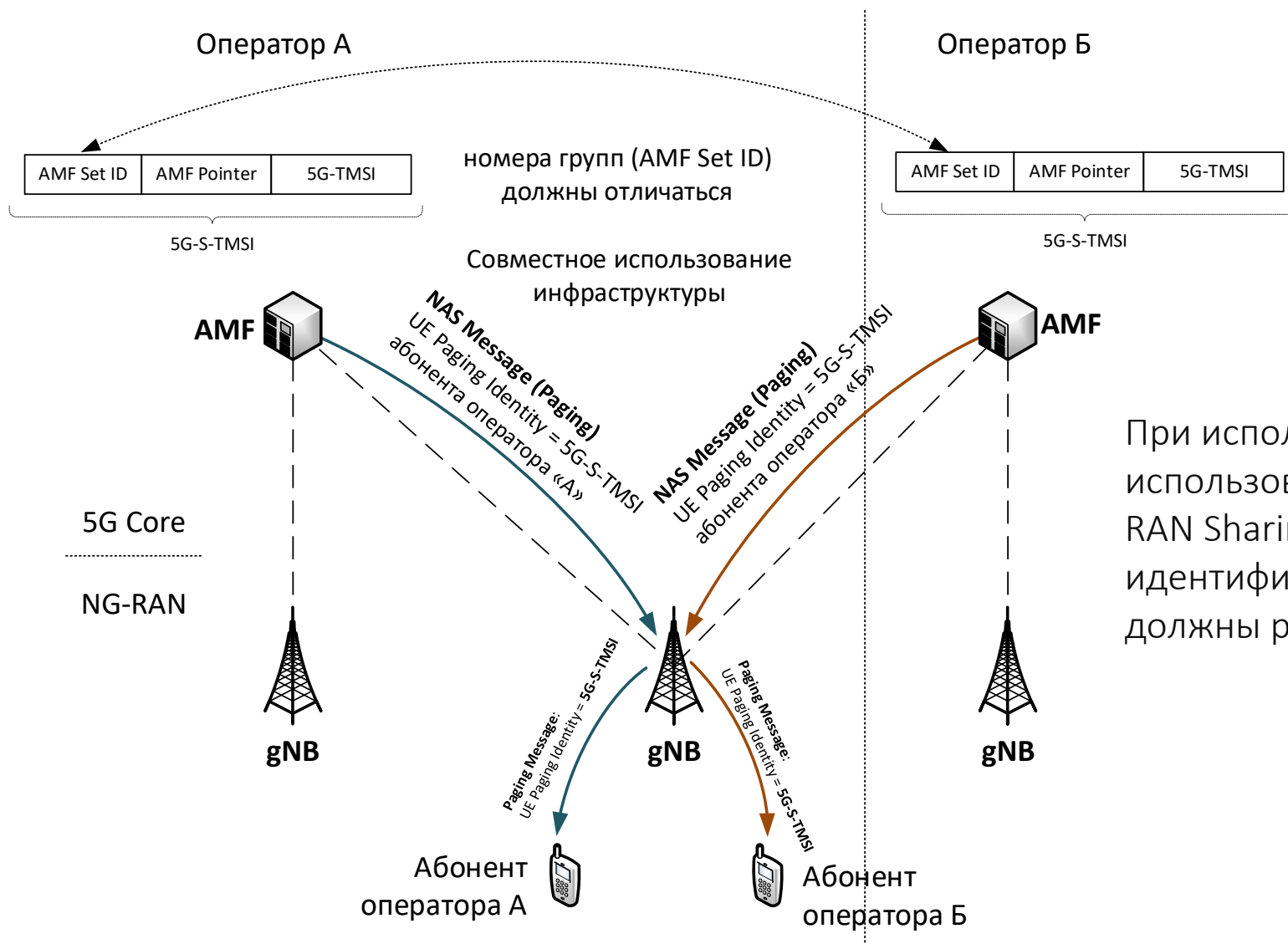
AMF Region ID – идентификатор региона, который обслуживается модулем AMF (0-255)

AMF Set ID – уникальный идентификатор подгруппы модулей AMF (0-1023)

AMF Pointer – уникальный идентификатор модуля AMF в группе AMF Set ID (0-63)

5G-TMSI (5G Temporary Mobile Subscription Identifier) – временный идентификатор мобильного абонента сети 5G (32 бита)

2. Нумерация и идентификация абонентского терминала в опорной сети 5GC



При использовании концепции совместного использования ресурсов сети радиодоступа RAN Sharing в целях исключения коллизий идентификаторы подгрупп AMF (AMF Set ID) должны распределяться между операторами

2. Нумерация и идентификация абонентского терминала в опорной сети 5G

3. Постоянный идентификатор оборудования абонентского терминала PEI (Permanent Equipment Identifier)

PEI является уникальным идентификатором оборудования абонентского терминала (АТ), осуществляющего доступ в сеть 5G. Идентификатор PEI может иметь несколько форматов: **IMEI** или **IMEISV**.



TAC (Type Allocation Code) – код модели и места производства абонентского терминала

SNR (Serial Number) – серийный номер абонентского терминала

Check Digit (CD) / Spare Digit (SD) – контрольная цифра (алгоритм Луна) / резерв

Контрольная цифра предназначена для предотвращения ошибок передачи IMEI вручную, например, когда абоненты регистрируют украденные АТ.

SVN (Software Version Number) – номер версии программного обеспечения

Контрольная цифра Check Digit используется, например, для контроля верности устной передачи идентификатора IMSI от абонента оператору

2. Нумерация и идентификация абонентского терминала в опорной сети 5GС

3. Постоянный идентификатор оборудования абонентского терминала PEI (Permanent Equipment Identifier)

Узнать свой IMEI или IMEISV: набрать на телефоне/смартфоне команду *#06#.

Проверить параметры на сайте, например, imei.info

The screenshot displays the imei.info website interface. The browser address bar shows the URL: `imei.info/?imei=356555084407710`. The page header includes navigation links: CHECK IMEI, IMEI CHECKER, IMEI CALCULATOR, FAQ, CARRIERS DATABASE, PHONE DATABASE, NEWS, and a LOG IN button. The main content area is divided into several sections:

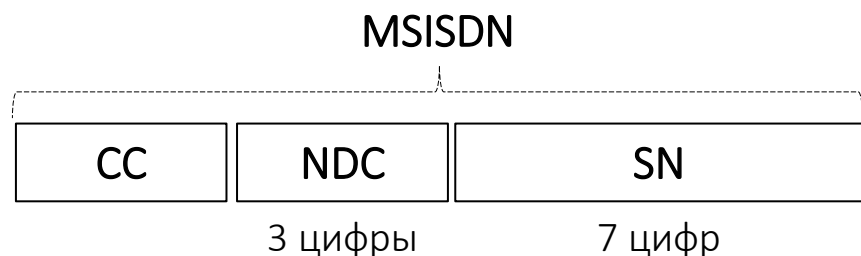
- Device Information:**
 - Brand: APPLE
 - IMEI: TAC: 356555 FAC: 08 SNR: 440771 CD: 0
 - More DETAILS... button
- Device Specifications:**
 - Device type: Smartphone
 - Design: Classic
 - Released: 2016 r.
 - SIM card size: Nano Sim
 - GSM: ✓850 900 1800 1900
 - HSDPA: ✓850 900 1900 2100 HSPA+
 - LTE: ✓LTE-FDD: 700, 800, 850, 900, 1700/2100, 1800, 1900, 2100, 2600
 - Dimensions (H/L/W): 138.3 x 67.1 x 7.1 mm, vol. 65 cm³
 - Display: RETINA Color (16M) 750x1334px (4.7") 326ppi
 - Touch screen: ✓
 - Weight: 138 g
 - Time GSM (talk/stand-by): 12 / 240 hrs. (10.0d)
 - Battery: Li-Po 1960 mAh
 - Non-removable battery: ✓
 - Built-in memory: ✓128 GB
 - RAM Memory: 2 GB
 - OS: iOS
 - Chipset: Apple A10 Fusion APL1W24
 - CPU #1 freq.: 2370.0 MHz (4-core)
- FREE CHECKS:**
 - Apple Warranty & Basic Info
 - Blacklist Simple Check
 - CHECK PHONE NUMBER
 - Check Serial Number
- PAID CHECKS:**
 - Carrier & Lock Status & FMI
 - Phone Blacklist Check PRO
 - Sim-Lock Status
 - Find My iPhone & iCloud Status
- Apple More Information:**
 - SN: 1CXXXXXXH67K
 - Color: Black
 - Memory: 128GB
 - Production date: 03-07-2018
 - iPhone age: 1 year(s), 3 month(s), 14 day(s)
 - Factory: China (Shenzhen)
 - Estimated purchase date: 14-09-2017
 - Apple Model Family Number: A1778
 - Apple Model Machine ID: iPhone9,3
 - Bootrom: 2696.0.01.33
 - Apple Model FCC ID 1: BCG-E3091A
 - Model Launched: 07-09-2016
 - Platform: t8010
 - CPID: 32784
 - BDID: 12

The bottom of the page shows a Windows taskbar with the system clock at 15:09 on 17.10.2019. A small notification bubble with the number 26 is visible in the bottom right corner of the taskbar.

3. Нумерация и идентификация абонентского терминала в подсистеме IMS

GPSI (Generic Public Subscription Identifier) – международный идентификатор подписки абонента на публичные сервисы сети 5G (например, сервисы подсистемы IMS)

Формат записи GPSI - телефонный номер абонента **MSISDN (Mobile Subscriber ISDN number)**



CC (Country Code) – телефонный код страны (+7 для России)
NDC (National Destination Code) – код направления или код сети
SN (Subscriber Number) – номер абонента

Например: MSISDN = +7 XXX 5105555

коды **DEF** для сетей мобильной связи (например, 903, 916, 925)

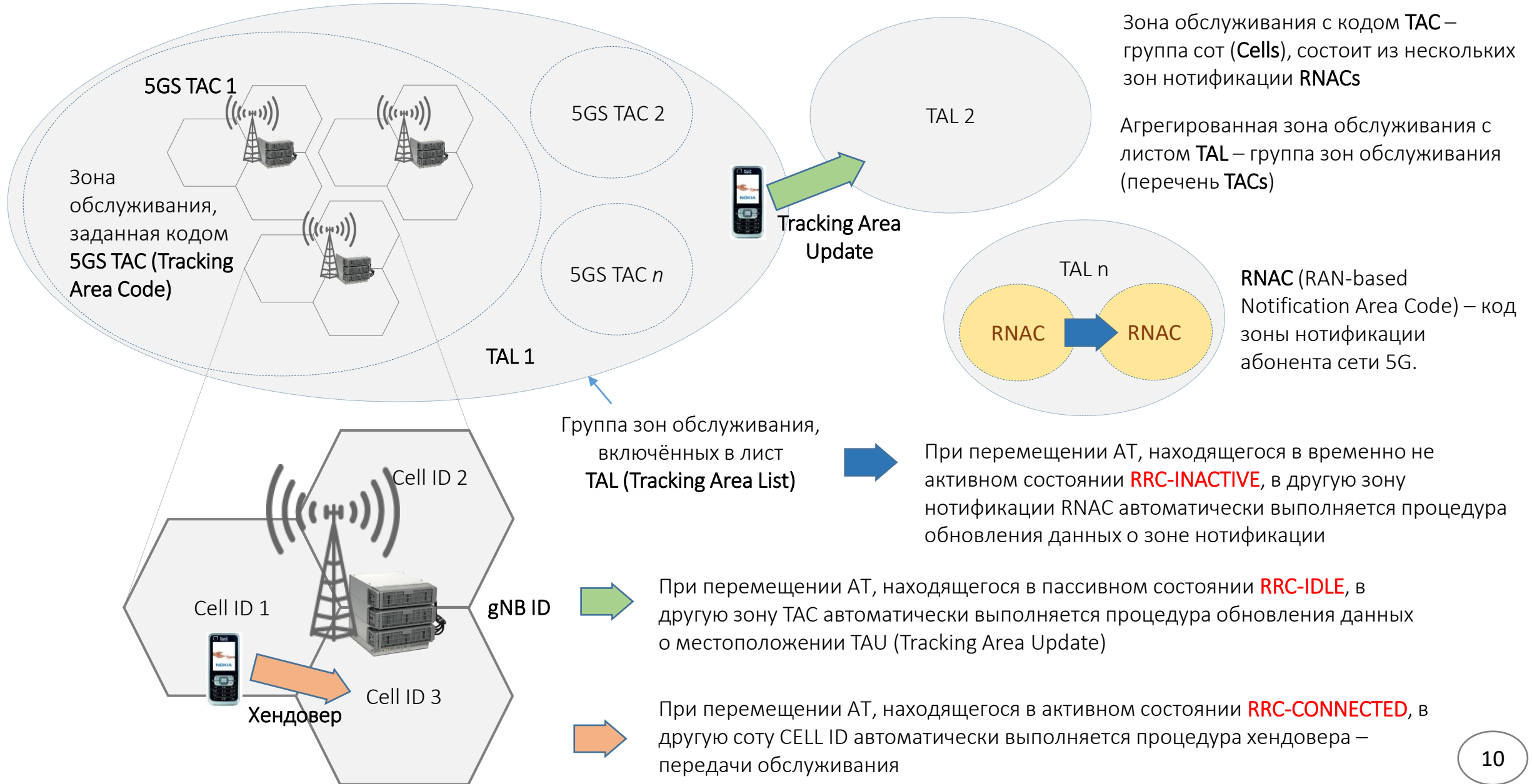
В сетях фиксированной телефонной связи – это коды **ABC** (например, 495, 499)

+7 ABC 5105555 – ISDN номер «домашнего» телефона

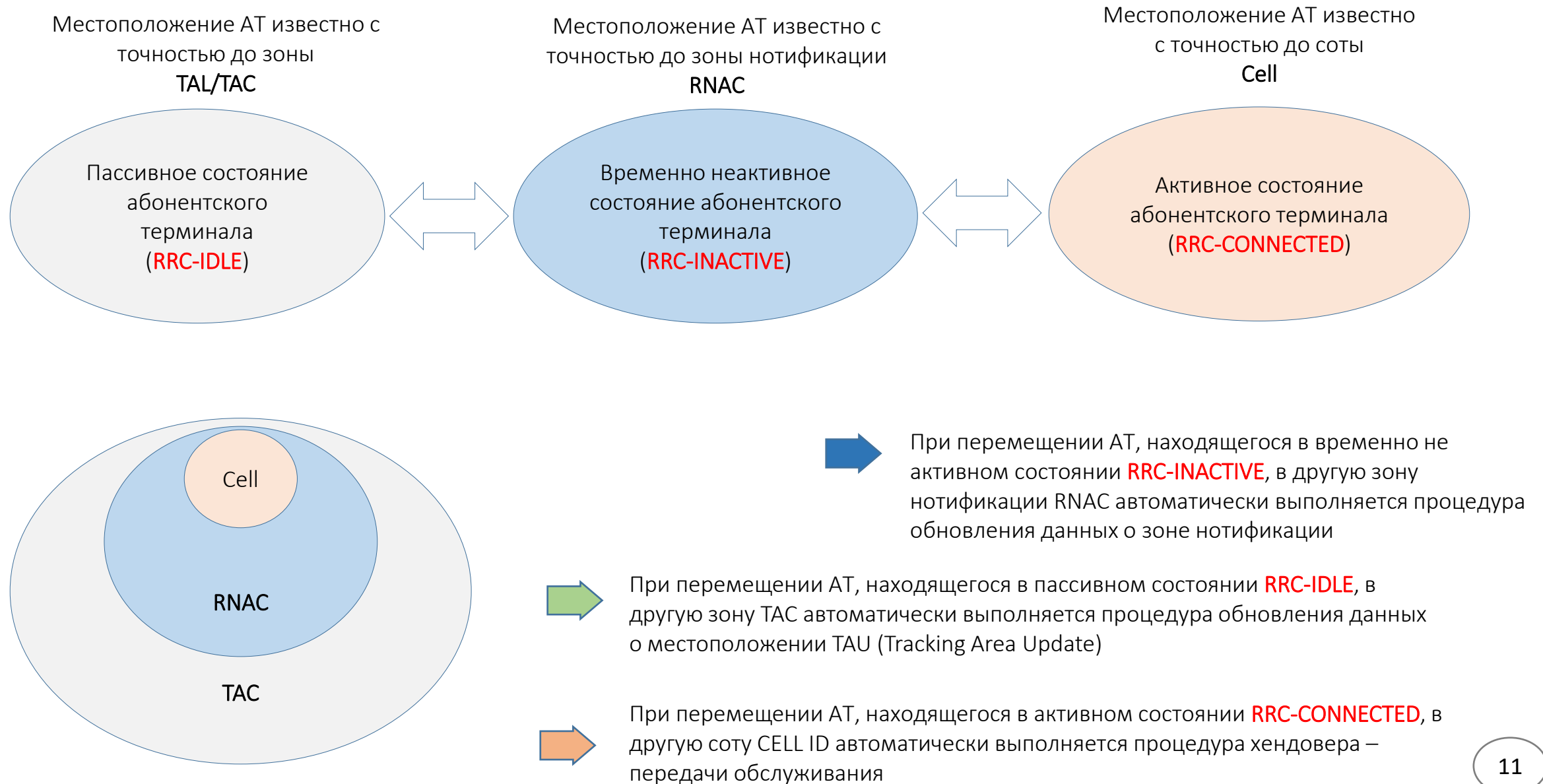
ABC – географически привязанная нумерация
DEF – географически не привязанная нумерация

+7 DEF 5105555 – MSISDN номер «сотового» телефона

4. Идентификация, используемая в сети радиодоступа NG-RAN

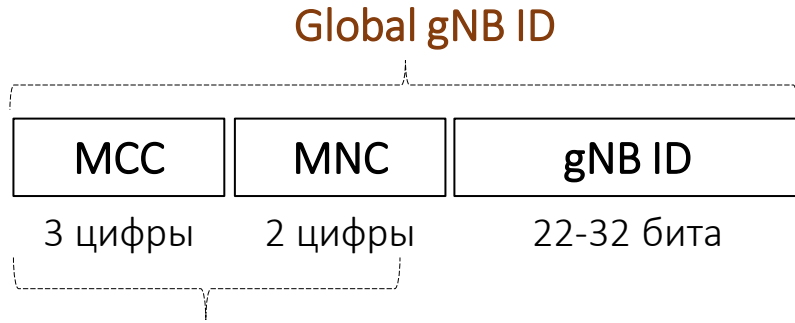


4. Идентификация, используемая в сети радиодоступа NG-RAN



4. Идентификация, используемая в сети радиодоступа NG-RAN

1. Международный идентификатор базовой станции Global gNB ID – уникальный международный идентификатор базовой станции, включает в свой состав коды MCC, MNC и идентификатор базовой станции gNB ID.



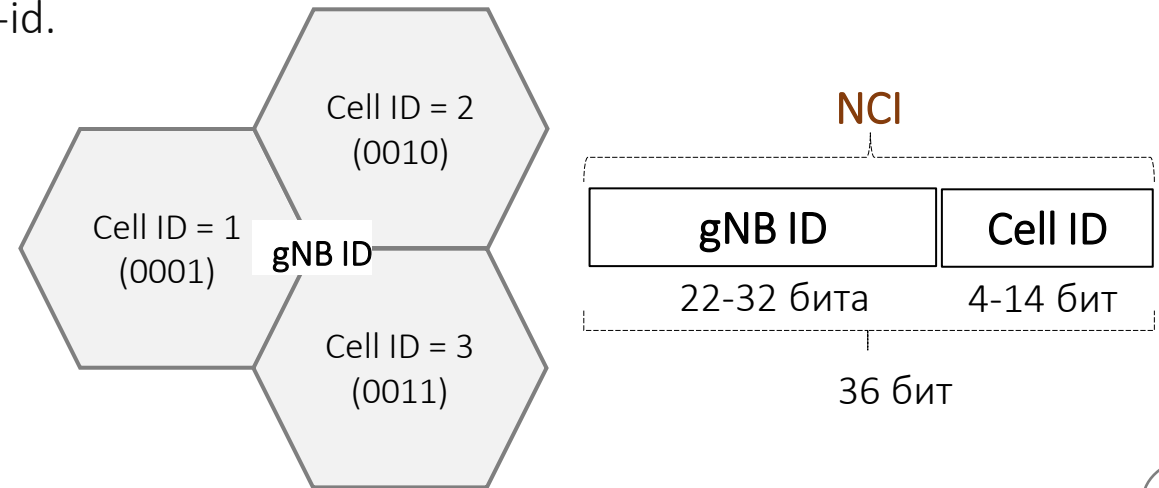
gNB ID – входит в состав идентификатора соты **NCI**, изменяется в пределах:

- 0 - 4 194 303 при длине идентификатора в 22 бита;
- 0 - 4 294 967 293 при длине идентификатора в 32 бита.

PLMN-id – идентификатор сети мобильной связи

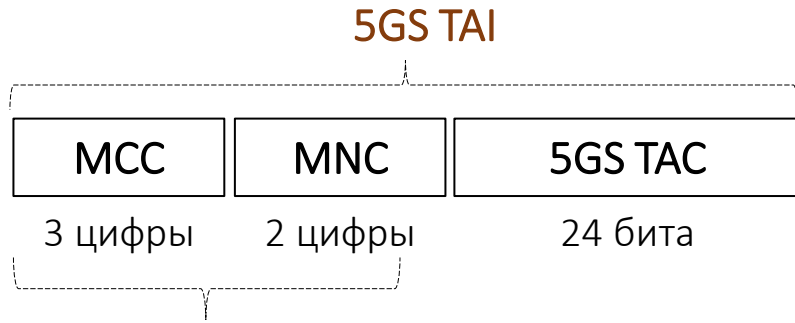
2. Идентификатор соты **NCI (NR Cell Identity)** – включает в свой состав идентификатор базовой станции gNB ID и идентификатор соты Cell Identity: **<NCI> := <gNB ID> <Cell Identity>**.
Идентификатор соты NR уникален в пределах сети PLMN-id.

3. Уникальный международный идентификатор соты **NCGI (NR Cell Global Identity)**:
<NCGI> := <MCC> <MNC> <NCI>.



4. Идентификация, используемая в сети радиодоступа NG-RAN

4. 5GS TAI (5GS Tracking Area Identity) – международный идентификатор зоны местоположения абонента, находящегося в состоянии RRC-IDLE.



PLMN-id – идентификатор сети мобильной связи

Пример:

5GS TAC = 7700120 (10)

5GS TAC = 01110101 01111110 10011000 (2)

TAC-low-byte = 10011000 (2) или 98 (16)

TAC-middle-byte = 01111110 (2) или 7e (16)

TAC-high-byte = 01110101 (2) или 75 (16)

5GS TAI FQDN = tac-lb98.tac-mb7e.tac-hb75.5gstac.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

5. 5GS TAI FQDN – полное доменное имя зоны местоположения:

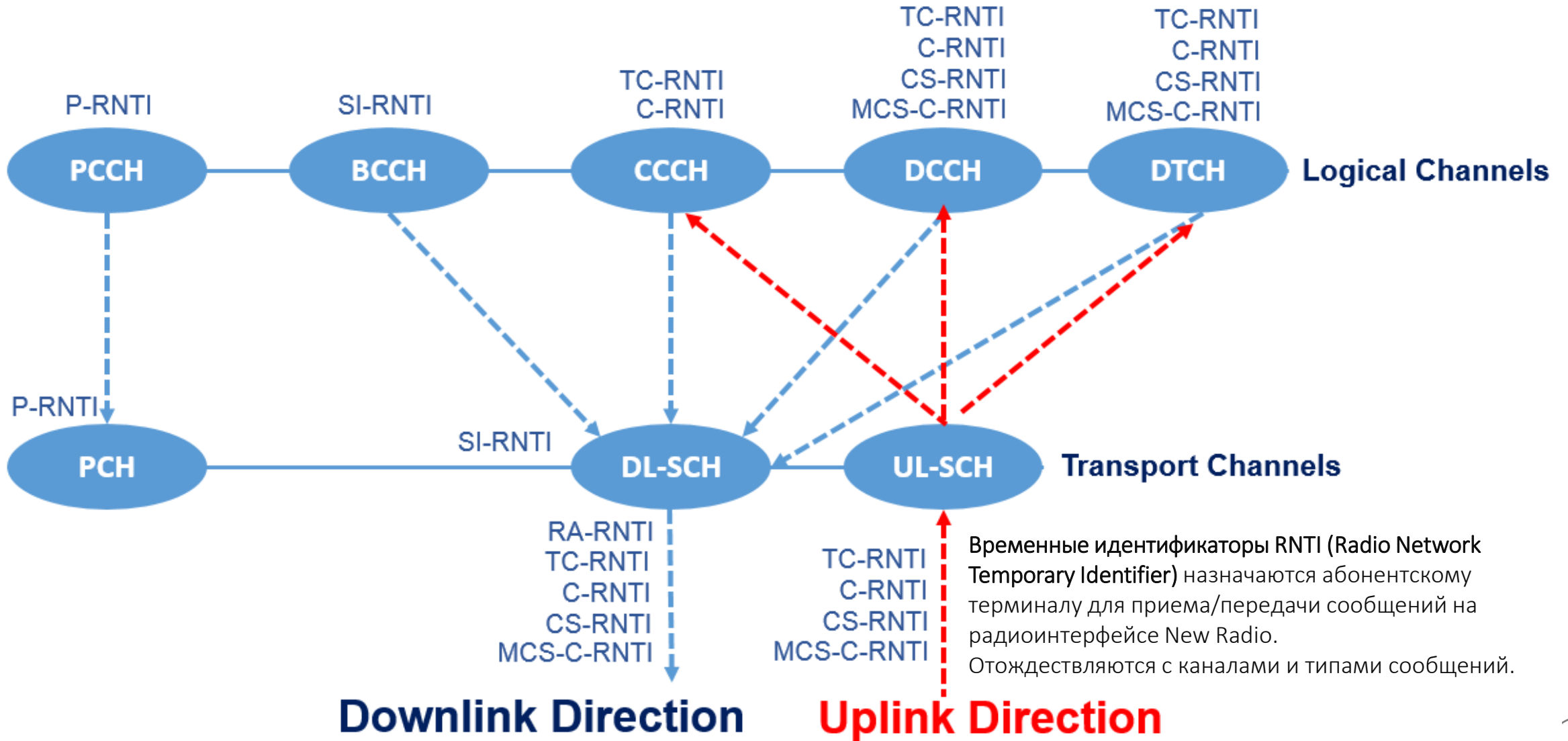
"tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

6. RNAC (RAN-based Notification Area Code) – код зоны нотификации абонента сети 5G, находящегося в состоянии RRC-INACTIVE, изменяется в пределах 0-255.

7. NR PCI (Physical Cell Identifier) – идентификатор физической соты NR, изменяется в пределах 0-1007. Определяет параметры первичного/вторичного (PSS/SSS) каналов синхронизации, излучаемых базовой станцией gNb в соте NR

4. Идентификация, используемая в сети радиодоступа NG-RAN

5. Временные идентификаторы AT в сети радиодоступа NG-RAN - RNTI



4. Идентификация, используемая в сети радиодоступа NG-RAN

5. Временные идентификаторы АТ в сети радиодоступа NG-RAN - RNTI

RNTI (Radio Network Temporary Identifier) – назначаемые абонентскому терминалу для приема/передачи сообщений на радиоинтерфейсе New Radio

SI-RNTI System Information RNTI. Общий в соте.	Общий широковещательный идентификатор для всех АТ в соте, используемый базовой станцией для передачи системной SI (System Information). Имеет длину 16 бит и изменяется в пределах 0-65535 (0xFFFF). Один идентификатор SI-RNTI используется для передачи всех системных информационных блоков SIBs логического широковещательного канала BCCH, передаваемых транспортным каналом DL-SCH, физическим каналом PDSCH.
P-RNTI Paging RNTI. Общий в соте.	Общий идентификатор для всех АТ в соте, идентификатор P-RNTI используется базовой станцией для обозначения сообщений пейджинга, передачи уведомлений об изменении системной информации SI, передачи коротких сообщений в соте (Short Message) . Имеет длину 16 бит и изменяется в пределах 0-65535 (0xFFFF). Используется в логическом канале пейджинга PCCH, транспортном канале пейджинга PCH, физическом канале PDSCH.
RA-RNTI Random Access RNTI. Индивидуальный для АТ.	Временный идентификатор RA-RNTI, назначаемый абонентскому терминалу в процессе выполнения процедуры конкурентного доступа в сеть 5G . Формируется протоколом MAC базовой станции gNB и передаётся в ответе за запрос доступа RAR (Random Access Response).
TC-RNTI Temporary Cell RNTI. Индивидуальный для АТ.	Временный идентификатор TC-RNTI, назначаемый абонентскому терминалу базовой станцией в сообщении RAR при выполнении процедуры конкурентного доступа в сеть 5G. Идентификатор TC-RNTI используется абонентским терминалом только во время выполнения процедуры доступа в сеть для скремблирования сообщения msg3 (RRCSetupRequest) .

4. Идентификация, используемая в сети радиодоступа NG-RAN

5. Временные идентификаторы АТ в сети радиодоступа NG-RAN - RNTI

C-RNTI Cell RNTI. Индивидуальный для АТ.	Идентификатор C-RNTI назначается абонентскому терминалу индивидуально в соте. Идентификатор C-RNTI используется для передачи сообщений протокола RRC для управления ресурсами линий UL и DL, отождествления передачи в каналах PUSCH, PUCCH с абонентским терминалом.
MCS-C-RNTI Modulation Coding Scheme Cell RNTI. Индивидуальный для АТ.	В сети 5G предусмотрено несколько схем модуляции и кодирования. Идентификатор MCS-C-RNTI назначается абонентскому терминалу для определения используемой таблицы модуляции и кодирования.
CS-RNTI Configured Scheduling RNTI. Индивидуальный для АТ.	В сети 5G предусмотрено несколько способов распределения сетевых ресурсов. Для передачи интерактивного голоса горизонт планирования радиоресурсов выше и распределение ресурсов выполняется на полупостоянной основе (Semi-Persistent). Идентификатор CS-RNTI назначается абонентскому терминалу для управления радиоресурсами на полупостоянной основе.
TPC-PUCCH-RNTI Transmit Power Control- PUCCH – RNTI. Уникальный для АТ.	Идентификатор TPC-PUCCH-RNTI назначается абонентскому терминалу для передачи сообщений управления мощностью передачи в линии «вверх». Идентификатор TPC-PUCCH-RNTI – для управления мощностью передачи в канале PUCCH. Идентификатор TPC-PUSCH-RNTI – для управления мощностью передачи в канале PUSCH. Идентификатор TPC-SRS-RNTI – для управления мощностью передачи опорного сигнала SRS.

4. Идентификация, используемая в сети радиодоступа NG-RAN

5. Временные идентификаторы AT в сети радиодоступа NG-RAN - RNTI

INT-RNTI Interruption RNTI. Индивидуальный для AT.	Идентификатор INT-RNTI, назначается абонентскому терминалу, находящемуся во временно не активном состоянии RRC-INACTIVE. Идентификатор INT-RNTI идентифицирует контекст AT в состоянии RRC-INACTIVE.
SFI-RNTI Slot Format Indication RNTI. Индивидуальный для AT.	В сети 5G предусмотрено несколько форматов слотов. Идентификатор SFI-RNTI определяет используемый формат тайм-слота.
SP-CSI-RNTI Semi-Persistent CSI RNTI. Индивидуальный для AT.	Идентификатор SFI-RNTI используется для передачи отчётов в канале PUSCH с низкой периодичностью (на полупостоянной основе) о текущем состоянии условий радиоприёма CSI (Channel State Information).

5. Идентификация, используемая в опорной сети 5GC

1. Доменные имена сетевых функций - мастер зона DNS домашней сети (Home Network Domain):

`5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

2. N3IWF FQDN (Fully Qualified Domain Name) – полное доменное имя сетевой функции N3IWF, имеет три формата обозначения:

✓ В привязке к сети оператора:

`n3iwf.5gc.mnc012.mcc345.pub.3gppnetwork.org`

✓ В привязке к зоне местоположения TAC и сети оператора:

`tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`

✓ В привязке к роумингу:

`n3iwf.5gc.mcc<MCC>.visited-country.pub.3gppnetwork.org`

3. NRF FQDN – полное доменное имя сетевой функции NRF в формате:

`nrf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

4. AMF FQDN – полное доменное имя сетевой функции AMF в формате:

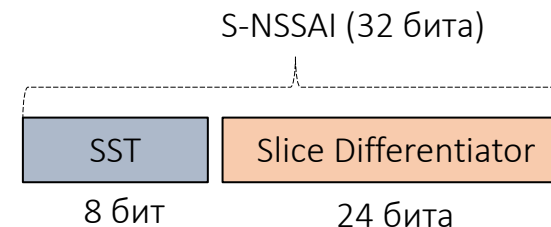
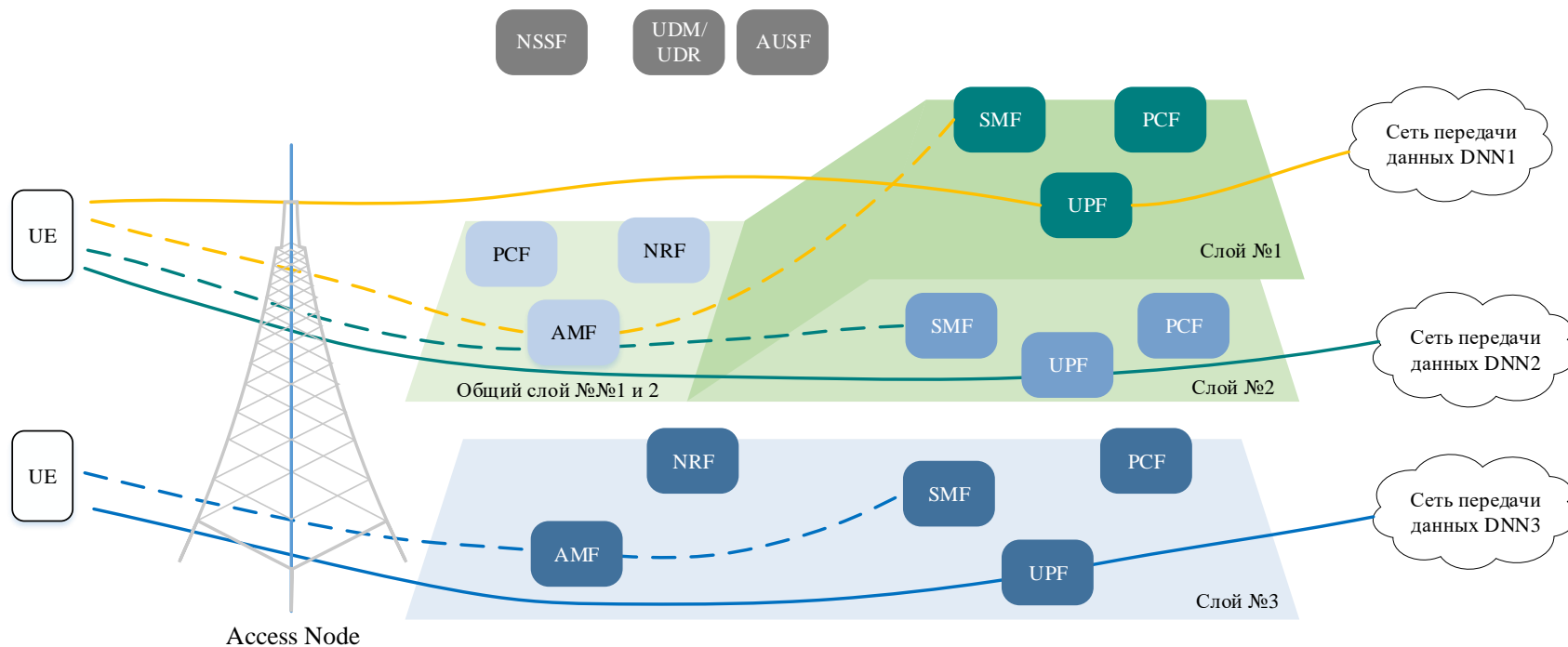
`AMF-id>.amf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

5. Идентификация, используемая в опорной сети 5GC

5. Сетевые слои Slices

S-NSSAI (Single Network Slice Selection Assistance Information) – информация о сетевом слое:

- тип сетевого слоя SST (Slice/Service type)
- отличительный признак сетевого слоя SD (Slice Differentiator)

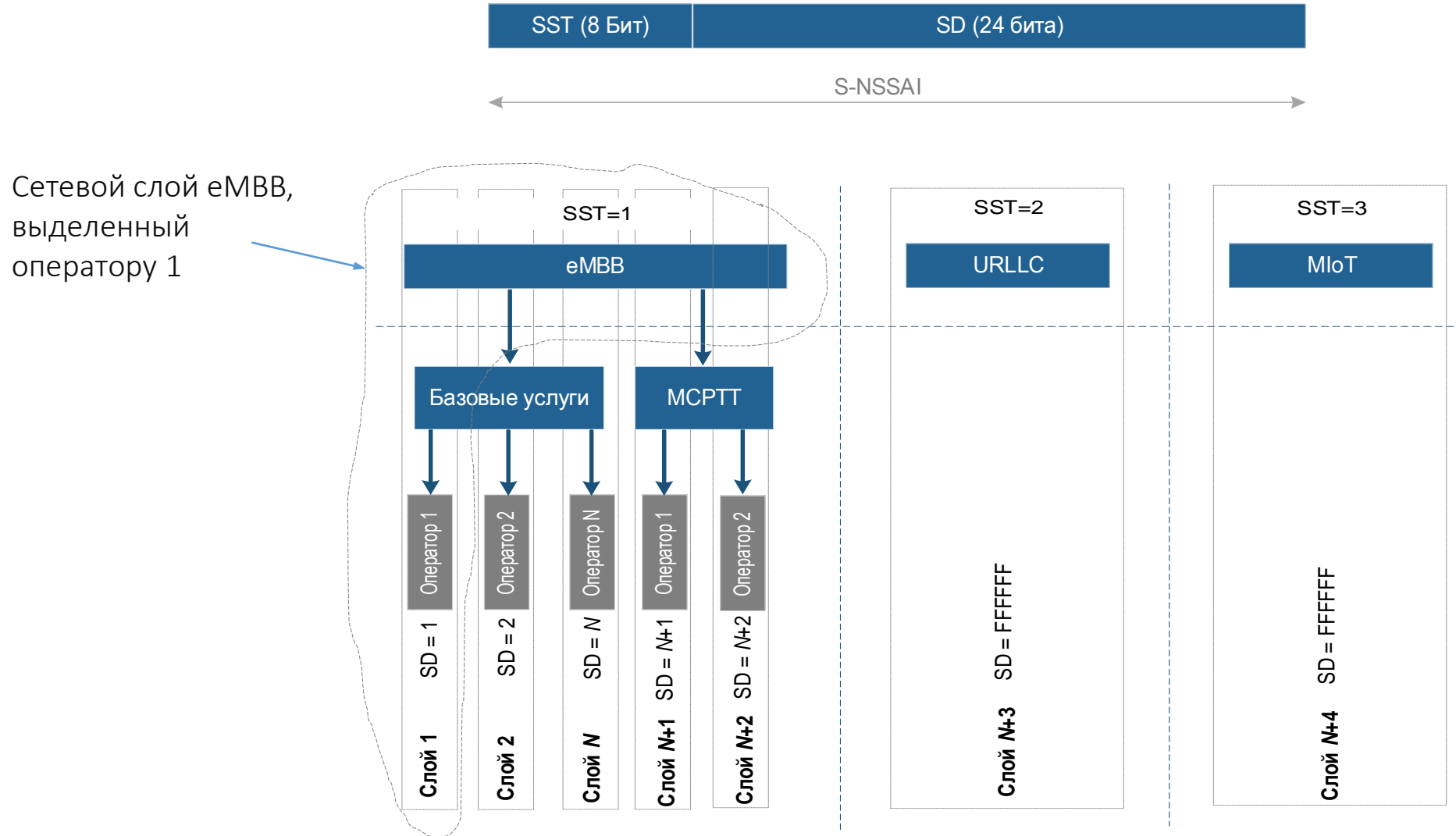


Сетевые слои, требуемые для оказания услуг 5G:

- сетевой слой мобильного широкополосного доступа eMBB (SST = 1)
- сетевой слой услуг с ультрамалыми задержками URLLC (SST = 2)
- сетевой слой массовых услуг Интернет-вещей MlIoT (SST = 3)

5. Идентификация, используемая в опорной сети 5GC

5. Сетевые слои Slices



5. Идентификация, используемая в опорной сети 5GC

6. IP-адресация

AS	Публичная автономная система пакетной транспортной сети. Изменяется в диапазонах 1-64495, 65522-4294967295.	До 10 цифр (decimal) или до 32 бит (RFC 1930, 4893)
	Приватная автономная система пакетной транспортной сети. Изменяется в диапазоне 64512-65534 . Диапазон 64496 – 64511 зарезервирован для использования в документации и примерах. Номера 0 и 65535 зарезервированы IANA и не используются в маршрутизации.	
Public IPv4	Публичные IPv4-адреса, динамически назначаемые абонентам и используемые трансляторами сетевых адресов NAT.	32 бита (RFC 791)
	Публичные IPv4-адреса, статически назначаемые абонентам.	
	Публичные IPv4-адреса, используемые на стыке пакетных транспортных сетей операторов.	
	Публичные IPv4-адреса, используемые на стыке пакетной транспортной сети с Интернет сервис-провайдерами (ISP).	
Local IPv4	Локальные IPv4-адреса, используемые закрытым сегментом пакетной транспортной сети, транспортными протоколами TNL сетевых функций сети 5G/IMT-2020. Например, пул адресов 10.0.0.0 – 10.255.255.255 .	
	Локальные IPv4-адреса, используемые для адресации PDU-сессии типа IPv4.	
	Например, пулы адресов 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255 .	

5. Идентификация, используемая в опорной сети 5GC

6. IP-адресация

Public IPv6	Глобальные индивидуальные IPv6-адреса из пула 2000::/3, назначаемые абонентам.	128 бит (RFC 2373)
	Глобальные индивидуальные IPv6-адреса из пула 2000::/3, используемые на стыке пакетных транспортных сетей операторов	
	Глобальные индивидуальные IPv6-адреса из пула 2000::/3, используемые на стыке пакетной транспортной сети с Интернет сервис-провайдерами (ISP)	
Local IPv6	Локальные IPv6-адреса, используемые закрытым сегментом пакетной транспортной сети, транспортными протоколами TNL сетевых функций сети 5G/IMT-2020: fc00::/7 – локальные индивидуальные IPv6-адреса; fe80::/10 – локальные индивидуальные IPv6-адреса (RFC 4291), автоматически назначаемые интерфейсам (не используются для целей маршрутизации пакетов данных). FF02::1, FF02::2 – групповые широковещательные адреса (RFC 4291).	