Reduced capability support

Reduced Capability (RedCap) is a 5G standard designed for UEs that do not require the full capabilities of 5G.

Table 1: Feature history

Feature name	Release information	Description
Event exposure service for UE reachability	2026.01.0	This feature enhances the Reduced Capability functionality by allowing the SMF to subscribe to the event exposure notification from AMF. The event exposure notification informs the SMF when the RedCap UE is reachable. **Commands enhanced:** • **service name type namf-evts**—Subscribes to AMF's event exposure service. • **message type AmfCreateEvtSubscription**—Configures the failure handling action for AmfCreateEvtSubscription message type. • **actiondef** *actdef_name* **priority** *priority_val* **action subscribe-ue-reachability**—Enables UE reachability subscription. **Default settings:**Disabled-Configuration required to Enable

Feature name	Release information	Description
Reduced Capability support on SMF	2025.03.0	This feature enables the SMF to support PDU sessions establishment over the RedCap RAT. SMF supports the connectivity of Reduced Capability UEs with the network by defining a new RAT type as RedCap. **Commands introduced:** • **user-plane-buffering-mgmt true** : Enables buffering at UPF. • **hlcom true** : Enables HLCOM sessions for entire DNN. • **policy extended-buffering** *extbuff* **{ sbpc** *sbpc_count* **ddnd** *ddnd_count* **| dbpc** *dbpc_count* **dbd** *dbd_duration* **}** : Configures the SBPC, DDND, DPDC, and DBD parameters. • **priority** *priority_val* **ruledef** *ruledef_name* **actiondef** *actdef_name* **event** *im-entry/paging_failure* : This CLI defines the event policy. • **ruledef** *ruledef_name* **condition { rat matches redcap | hlcom is true }** : This CLI defines the rule. • **actiondef** *actdef_name* **priority** *priority_val* **action extended-buffering attributes policy** *extbuff* : This CLI defines the action. **Default settings:**Disabled-Configuration required to Enable

Reduced Capability

The RedCap UEs, such as wearables and industrial sensors, typically operate in low-power or idle states and transition to the active state only when data transfer is needed. For the rest of the time, the RedCap UEs are either in power-saving mode or are unreachable.

High Latency Communication

When a RedCap UE enters the power-saving modes like "Power-Saving Mode (PSM)" or "Extended Idle Mode DRX (eDRX)", it becomes unreachable for a period, leading to high latency during the initial data exchange.

To mitigate this, the High Latency Communication (HLCOM) feature buffers Mobile Terminated (MT) data at the UPF, while the UE is in the power-saving state. This extended buffering ensures that the data is not lost and is available when the UE becomes reachable again.

The HLCOM is particularly beneficial for Machine Type Communication (MTC) devices (IoT devices) that frequently use PSM and eDRX to optimize energy consumption.

This feature allows the network operators to support the connectivity of RedCap UEs with the network by introducing a new RAT type in SMF, called as RedCap.

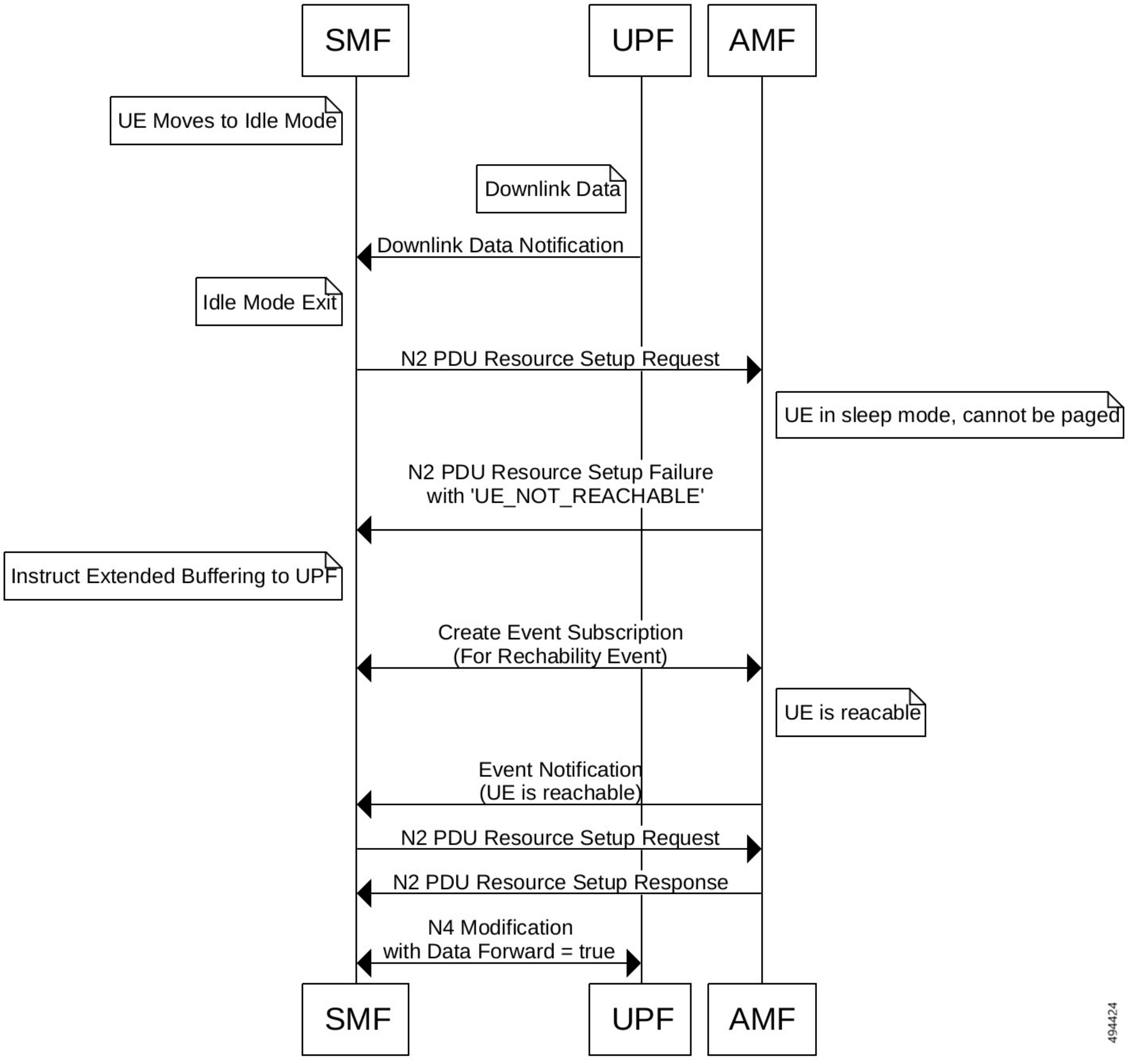
How RedCap Support works

Summary

This process explains the process in which Reduced Capability functionality works.

Workflow

Figure 1: Call flow for PDU Session Establishment for RedCap UEs


SMF
UPF
AMF
UE Moves to Idle Mode
Downlink Data
Downlink Data Notification
Idle Mode Exit
N2 PDU Resource Setup Request
UE in sleep mode, cannot be paged
N2 PDU Resource Setup Failure with 'UE_NOT_REACHABLE'
Instruct Extended Buffering to UPF
Create Event Subscription (For Rechability Event)
UE is reacable
Event Notification (UE is reachable)
N2 PDU Resource Setup Request
N2 PDU Resource Setup Response
N4 Modification with Data Forward = true
SMF
UPF
AMF
494424

Note For this feature to work

- HLCOM should be enabled on SMF. For more details on the HLCOM configuration, see the Enable HLCOM for a RedCap session section.
- The compliance profile should be configured with v17.5.0 for the service **nsmf-pdusession**.

These stages explain the process of RedCap support on SMF:

1. **RedCap PDU Session Establishment:** A RedCap UE sends a PDU Session Establishment Request to AMF.

Upon receiving the request, AMF sends a PDU Session SM Context Request to SMF and sets the **ratType IE** as **RedCap** in the message.

2. **Subscription, policy creation, and charging data requests:** SMF receives the ratType IE as RedCap from AMF and forwards it to UDM, PCF, and CHF for subscription, policy creation, and charging data requests respectively.

3. **BAR creation during N4 Session Establishment:** The buffering duration and packet count for HLCOM are communicated from the SMF to the UPF using Buffering Action Rules (BARs) as defined in the 3GPP TS 29.244 specification.

   SMF sends the N4 Session Establishment Request to the UPF including the ratType IE as RedCap. SMF also creates an empty BAR and associates it to the FARs during N4 Session Establishment.

4. **UE's entry in the Idle mode:** SMF instructs the UPF to buffer when the UE moves to idle state. SMF sends an N4 Session Modification Request to UPF with UpdateBAR IE containing these IEs:

   Table 2: Buffering IEs in UpdateBAR IE

Buffering IE	Description
DDND (Downlink Data Notification Delay)	The UP function supports the buffering parameter "Downlink Data Notification Delay (DDND)".
SBPC (Suggested Buffering Packets Count)	The UP function supports the "Suggested Buffering Packets Count (SBPC)" is present, when the UP function indicates the support of the feature UL/DL Buffering Control (UDBC).

   UPF sends the Downlink Data Notification to SMF.

5. **UE's exit from the Idle mode:** SMF sends an N1 N2 Transfer Request to AMF. SMF sets the **extBufSupport IE** (Extended Buffering Support) to true in the N2 PDU Setup Request message to indicate extended buffering support to AMF based on configuration and based on the UPF support.

   SMF does not set extBufSupport to true in case of paging for a control plane message.

   As the UE is unreachable, the AMF sends a PDUSessionResourceSetupRequestTransfer Response message to SMF including the status code and cause as **504: UE_NOT_REACHABLE**. SMF also receives a **maxWaitingTime IE** (Estimated Maximum Waiting Time) in the **N1N2MsgTxfrErrDetail IE**. SMF starts the **maxWaitingTime IE** timer and stores the flow information for retry.

   SMF sends the N4 Modification Request with UpdateBAR with "**DL Buffering Duration (DBD)**" same as the estimated maximum wait time and "**DL Buffering Suggested Packet Count (DBPC)**" from the configuration, if the UPF has indicated the support for DBDM.

6. **Subscription to UE reachability Notification:** SMF subscribes to AMF's CreateEventSubscriptions, when it receives the error **504: UE_NOT_REACHABLE** from the AMF. The subscription includes the event types as **REACHABILITY_REPORT** and reachability filter as **UE_REACHABLE_DL_TRAFFIC**, if the configuration is present.

   For more details on the configuration, see the Configure HLCOM RedCap sessions section.

7. **UE reachable:** SMF receives the event notification from the AMF, once the UE is reachable again. This notification includes a UE Reachability filter as **Reachable**.

SMF extracts the QCI and ARP values from the flow that is marked as **awaiting_reachability**. When the UE moves to the active state, the status is reset.

SMF sends the N1N2 Transfer Request containing N2 Setup Request, to AMF.

AMF sends a N2 Setup Request to the gNB. The gNB sends N2 Setup Response. SMF sends the N4 Modification Request to the UPF.

Note In case of AMF change, the N1N2 Transfer Request should happen before the event subscription. Therefore, even during AMF change, it does not require any additional change for event exposure discovery.

Selection of AMF address for event exposure

SMF uses these two methods to determine the AMF's address for event exposure:

- **NRF-based AMF discovery:** SMF selects the NF service with service name configured as **namf-evts** and selects the peer address from NF service.

  In case SMF does not find the matching NF service, it selects the peer address from the NF client profile configuration.

- **NF client profile configuration:** SMF uses the AMF's IP address configured under the NF client profile corresponding to the AMF event exposure service to determine the AMF.

  To see the NF client profile configuration, see the Subscribe to AMF's Event Exposure service.

Limitations

These are the known limitations of Reduced Capability support on SMF:

- 17.x compliance profile is required for **nsmf-pdusession**, **npcf-smpolicycontrol**, and **chf-convergedcharging** services.
- 16.9.x compliance profile is required for **namf-comm** services.
- SMF supports the extended buffering (HLCOM) functionality only for the RedCap RatType and not for other RatTypes.
- SMF supports the extended buffering only for Idle mode exit due to data trigger.
- The RedCap PDU Session Establishment is not supported for roaming calls.
- UPF selection based on HLCOM supported feature bits is not supported.
- The AMF selection or discovery for **namf-comm** service based on HLCOM is not supported.
- SMF will cap the DBD value to a higher value in case of encoding restrictions on the N4 interface.
- The ratType label with NR_REDCAP value is not supported for **policy_msg_processing_status** stats.

Standards compliance

SMF supports 3GPP compliance profile version 17.5.0 for the service nsmf-pdusession, 17.15.0 for the npcf-smpolicycontrol, and 17.1.0 for chf-convergedcharging.

Enable RedCap support on SMF

Follow these steps to enable the RedCap support on SMF:

Procedure

Step 1 Enable HLCOM for a RedCap session.

Step 2 Configure buffering values for HLCOM RedCap sessions.

Enable HLCOM for a RedCap session

This configuration in DNN profile is used to send ExtBuffSupport in N1N2 message.

Follow these steps to enable the HLCOM for a RedCap session:

Procedure

Step 1 Use the CLI **profile dnn** *dnn_profile* to create an instance of the DNN profile.

Example:

```
[smf] smf# config
[smf] smf(config)# profile dnn data-hlcom
[smf] smf(config-dnn-data-hlcom)#
```

Step 2 Use the CLI **user-plane-buffering-mgmt true** to create BAR and link the FARs to it.

Example:

```
[smf] smf(config-dnn-data-hlcom)# user-plane-buffering-mgmt true
[smf] smf(config-dnn-data-hlcom)#
```

Step 3 Use the CLI **hlcom true** to send ExtBuffSupport IE in the N1N2 message. Save and exit from the current configuration mode.

Example:

```
[smf] smf(config-dnn-data-hlcom)# hlcom true
[smf] smf(config-dnn-data-hlcom)# exit
[smf] smf(config)#
```

What to do next

After enabling the HLCOM for a RedCap session, you must configure the buffering values for the HLCOM session. For more information on this, see the Configure buffering values for HLCOM RedCap sessions topic.

Subscribe to AMF's Event Exposure service

This task allows SMF to subscribe to the AMF's event exposure service.

Procedure

Step 1 Use the CLI **profile nf-client nf-type amf amf-profile** *profile_name* to create an instance of the peer AMF.

Example:

```
[smf] smf#config
[smf] smf(config)#profile nf-client nf-type amf
[smf] smf(config-amf)#amf-profile AP1
[smf] smf(config-amf-profile-AP1)#
```

Step 2 Configure the locality, priority values, and service type.

Example:

```
[smf] smf(config-amf-profile-AP1)#locality LOC1
[smf] smf(config-amf-profile-AP1)#priority 30
[smf] smf(config-amf-profile-AP1)#service name type namf-evts
```

Step 3 Configure the endpoint related values.

Example:

```
[smf] smf(config-amf-profile-AP1)#endpoint-profile EP2
[smf] smf(config-amf-profile-AP1)#uri-scheme http
[smf] smf(config-amf-profile-AP1)#endpoint-name EP1
[smf] smf(config-amf-profile-AP1)#priority 56
[smf] smf(config-amf-profile-AP1)#primary ip-address ipv4 10.1.43.44
[smf] smf(config-amf-profile-AP1)#primary ip-address port 9012
```

What to do next

In order to subscribe to the event exposure service from the AMF, configure the action management policy. For more information, see Configure HLCOM RedCap sessions.

Configure HLCOM RedCap sessions

These steps define the process of buffering values for HLCOM RedCap Sessions:

Before you begin

Before configuring the buffering values for HLCOM sessions, you must enable HLCOM. For more information on this configuration, see the Enable HLCOM for a RedCap session topic.

Procedure

Step 1 Use the CLI **policy extended-buffering** *extbuff* to create an instance of the Extended Buffering policy.

Example:

```
[smf] smf# config
[smf] smf(config)# policy extended-buffering buf1
[smf] smf(config-extended-buffering-buf1)#
```

Step 2 Use the CLIs **{ sbpc** *sbpc_count* **ddnd** *ddnd_count* **} { dbpc** *dbpc_count* **dbd** *dbd_duration* **}** to define the SBPC, DDND, DBPC, and DBD parameters. Save and exit the current configuration mode.

Example:

```
[smf] smf(config-extended-buffering-buf1)# sbpc 200 ddnd 1000
[smf] smf(config-extended-buffering-buf1)# dbpc 1000 dbd 30
[smf] smf(config-extended-buffering-buf1)# exit
[smf] smf(config)#
```

Note

SBPC and DDND values are used during the Idle mode entry. DBPC and DBD values are used during Idle mode exit.

Step 3 Use the CLI **policy eventmgmt** *eventmgmt_name* to create an instance of the Event Management policy.

Example:

```
[smf] smf(config)# policy eventmgmt Redcap
[smf] smf(config-eventmgmt-Redcap)#
```

Step 4 Use the CLI **priority** *priority_val* **ruledef** *ruledef_name* **actiondef** *actdef_name* **event** *im-entry/paging_failure* to define the ruledef and actiondef for the configured Event management policy. Save and exit the current configuration mode.

Example:

```
[smf] smf(config-eventmgmt-Redcap)# priority 1 event imentry ruledef rdRedcap actiondef
 adRedcap
[smf] smf(config-eventmgmt-Redcap)# priority 2 event paging-failure ruledef rdRedcap
actiondef adRedcap
[smf] smf(config-eventmgmt-Redcap)# exit
[smf] smf(config)#
```

Step 5 Use the CLI **policy rulemgmt** *rulemgmt_name* to create an instance of the Rule Management policy.

Example:

```
[smf] smf(config)# policy rulemgmt rm1
[smf] smf(config-rulemgmt-rm1)#
```

Step 6 Use the CLI **ruledef** *ruledef_name* **condition { rat matches redcap | hlcom is true }** to define the rule. Save and exit to the Global Configuration mode.

Example:

```
[smf] smf(config-rulemgmt-rm1)# ruledef rdRedcap
[smf] smf(config-ruledef-rdRedcap)# condition rat matches redcap
[smf] smf(config-ruledef-rdRedcap)# condition hlcom is true
[smf] smf(config-ruledef-rdRedcap)# exit
[smf] smf(config-rulemgmt-rm1)# exit
[smf] smf(config)#
```

Step 7 Use the CLI **policy actionmgmt** *actmgmt_name* to create an instance of the Action Management Policy.

Example:

```
[smf] smf(config)# policy actionmgmt ad1
[smf] smf(config-actionmgmt-ad1)#
```

Step 8 Use the CLI **actiondef** *actdef_name* **priority** *priority_val* **action { extended-buffering | subscribe-ue-reachability } attributes policy** *extbuff* to define the policy, extended buffering, and priority. Save and exit to the Global Configuration mode.

Example:

```
[smf] smf(config-actionmgmt-ad1)# actiondef adRedcap
[smf] smf(config-actiondef-adRedcap)# priority 1 action extended-buffering attributes
policy buf1
[smf] smf(config-actiondef-adRedcap)# priority 1 action subscribe-ue-reachability
[smf] smf(config-actiondef-adRedcap)# exit
[smf] smf(config-actiondef-adRedcap)# exit
[smf] smf(config)#
```

Configure failure handling template for AMF's Event Exposure service

This task allows you to configure the failure handling template for AMF's event exposure service.

Before you begin

Before configuring the failure handling template, you must subscribe to AMF's Event Exposure service. For more information, see the Configure HLCOM RedCap sessions.

Procedure

Step 1 Use the CLI **profile nf-client-failure nf-type amf** to create an instance of the peer AMF.

Example:

```
[smf] smf#config
[smf] smf(config)#profile nf-client-failure nf-type amf
[smf] smf(config-amf)#
```

Step 2 Use the CLI **profile failure-handling** *failure_handling_profile* to create a failure handling profile for AMF.

Example:

```
[smf] smf(config-amf)#profile failure-handling FHAMF
[smf] smf(config-failure-handling-FHAMF)#service name type namf-evts
```

Step 3 Use the CLI **message type** *message-type* to configure the message type in the event of the failure.

Example:

```
[smf] smf(config-failure-handling-FHAMF)#message type AmfCreateEvtSubscription
[smf] smf(config-failure-handling-FHAMF)#
```

Step 4 Configure status code, retry, and action for handling failure.

Example:

```
[smf] smf(config-failure-handling-FHAMF)#status-code httpv2 504
[smf] smf(config-failure-handling-FHAMF)#retry 1
[smf] smf(config-failure-handling-FHAMF)#action retry-and-continue
[smf] smf(config-failure-handling-FHAMF)#
```

Monitoring and troubleshooting

This section discusses the bulkstats and show commands used for monitoring and troubleshooting this feature.

Bulkstatistics

These are the statistics used to support this feature:

- The label **ratType** in all the existing stats reflect value the as **NR:Redcap** for Redcap sessions.
- The N4 message stats is enhanced to indicate BAR creation.

```
proto_udp_req_msg_total{app_name="SMF",
bar_present="true",cluster="SMF",
data_center="DC",gr_instance_id="1",instance_id="0",
interface_type="N4",message_direction="outbound",
message_name="session_establishment_req",
msgpriority="",peer_info="SMFIP:10.1.9.165:UPFIP:10.1.12.172",
sec_pdr_present="false",service_name="protocol1",
status="accepted",transport_type="origin"} 1
```

- To support the Event Exposure service for RedCap sessions, these labels are added in the **amf_event_exposure_stats** statistics:
  - **message_type**—AmfCreateEventSubscription, AmfEventNotification.
  - **ee_trigger_type**— ReachabilityReport, LocationReport
  - **status**— attempted, success, failed.
  - **dnn**— In order to display this label, it needs to enable it through **granular-labels [dnn]** CLI command under the smf_service_stats metrics profile.

    ```
    infra metrics verbose application
    metrics smf_service_stats
    granular-labels [ dnn ]
    exit
    ```

  - **snssai**
  - **rat_type**

This is the example of amf_event_exposure_stats:

```
amf_event_exposure_stats{app_name="SMF",
cluster="SMF",data_center="DC",dnn="intershat",
ee_trigger_type="ReachabilityReport",gr_instance_id="1",
instance_id="0",message_type="AmfCreateEventSubscription",
rat_type="NR_REDCAP",service_name="smf-service",snssai="",
status="attempted",status_code=""} 2
```

show subscriber namespace smf rat nr-redcap

The output of the show command **show subscriber namespace smf rat nr-redcap** is enhanced to support the RedCap functionality on SMF.

```
[smf] smf# show subscriber namespace smf rat nr-redcap"alwaysOn": "None",
        "dcnr": "None",
        "wps": "Non-Wps Session",
        "ratType": "NR_REDCAP",
        "ueType": "NR Capable UE",
        "iwkEpsInd": true,
        "sessTimeStamp": "2025-07-09 09:09:01.550487493 +0000 UTC",
        "callDuration": "5.471171384s",
        "ipPool": "poolv4DNN4",
        "commonId": 2097190,
        "linkedEbi": 6,
        "smfIwkEpsInd": true,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        "radiusEpInfo": "10.1.46.49:1812",
        "authAlg": "pap-default",
        "serverGroup": "radServerGrp",
        "authStatus": "Authenticated",
        "roamingStatus": "Homer",
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "ipAllocationBy": "Radius",
        "anType": "3GPP_ACCESS",
        "initialRatType": "NR_REDCAP"
      },
```