Analyses of CBCF – SCP in 5GC

FUDGE-5G Project Newsletter #5 February 2022

In a 5G Core, the Cell Broadcast Centre Function (CBCF) is an instantiation of an Application Function (AF) as specified in 3GPP Release-15. A CBCF uses the services of an Access and Mobility Function (AMF) and a Network Repository Function (NRF) for warning message delivery. In Release-16, the Service Communications Proxy (SCP) was introduced. If deployed, the SCP helps operators to efficiently secure and manage their 5G network by providing routing control, easy scalability, and delegated discovery to the core network. Here we analyse how the CBCF communicates with the core network in a Release-15 environment compared to a Release-16 environment where an SCP is present. After an explanation of the role of the CBCF and SCP in the 5G architecture, warning message delivery is described for an environment without an SCP present. Subsequently, the SCP is described followed by an explanation about warning message delivery in an environment in which an SCP is present.

The 5G system architecture is presented in Figure 1, with the network functions of relevance for this article marked in blue text. The main role of a CBCF is to initiate warning message delivery to UEs in an area. As shown in the 5G system architecture the CBCF uses the services of the AMF via the Namf reference point for delivery of warning messages to the RAN via the N2 reference point and cells in the warning area will broadcast the warning message. This warning message delivery is an unacknowledged broadcast service.

When the CBCF receives a request to initiate warning message broadcast (which is not shown in Figure 1), it first determines the list of cells that cover the target area of the warning message. The target area is for example provided as a polygon or a geo-code.

The CBCF needs to be provisioned with cell IDs, the coverage area of each cell, the Tracking Area ID that is configured for each cell and the AMF Set that serves the Tracking Area. Since cell information cannot be obtained from the core network the cell information has to be provisioned, but the AMF instances, AMF Sets and their Tracking Areas can also be discovered via the NRF.

Warning message delivery without SCP

Each RAN node (gNodeB or ng-eNodeB) has, upon deployment, registered with one or more AMFs and has indicated which Tracking Areas it supports. An AMF has registered itself with the NRF and provided the list of Tracking Areas that the AMF supports. The CBCF can discover the AMFs and the Tracking Areas they support via the

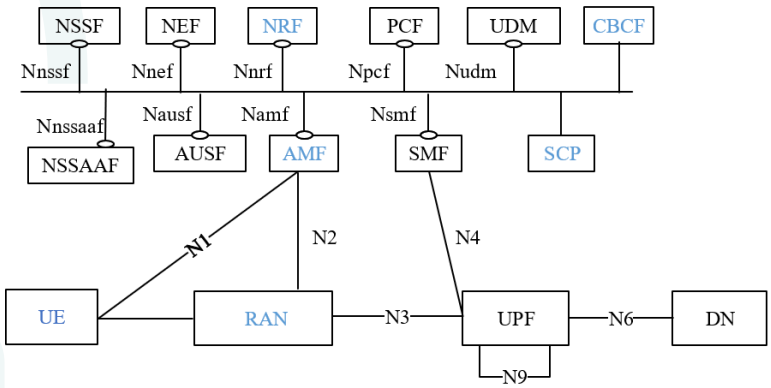


Figure 1: 5G System architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

Nnrf_NFDiscovery service provided by the NRF. Hence, the CBCF determines the AMF instance for warning message delivery to a particular area via the Tracking Area(s) the AMF supports. Alternatively, instead of discovery, also the AMFs and the Tracking Areas they serve can be provisioned in the CBCF, since cell provisioning will have to be done either way.

The CBCF uses the Namf_Communication service from the AMF for warning message delivery to the RAN via the N2 reference point for delivering a Write-Replace-Warning-Request-NG-RAN or to cancel warning message delivery by sending a Stop-Warning-Request-NG-RAN via the AMF to the same area as the Write-Replace-Warning-Request-NG-RAN was sent to. The CBCF selects an AMF instance in the AMF Set based on policy and AMF availability.

The CBCF subscribes to receive notifications on success or failure of broadcast and on restart and failure of cells. Cells that have failed to schedule broadcast successfully or cells where stopping the broadcast was unsuccessful may be retried by the CBCF. Cells that have restarted should possibly be reloaded by the CBCF. These subscriptions are held by each AMF instance individually since there is no mechanism to distribute subscriptions among AMF instances.

The CBCF subscriptions that are held in the AMF are deleted when the AMF restarts and the CBCF will need to renew these subscriptions. Furthermore, the CBCF will subscribe to notifications when a new AMF instance is deployed and needs to be used by the CBCF. Therefore, the CBCF uses the NFStatusSubscribe service from the NRF to receive notifications from the NRF about status changes of AMFs. Status change of an AMF could be: (de)registration of AMF; Profile change of an AMF, such as the recoveryTime (restart); Loss of subscriptions in the AMF.

Upon registration of an AMF, the CBCF is notified of: backupInfoAmfFailure indicates for which AMF this AMF serves as backup; backupInfoAmfRemoval indicates for which AMF that is planned for removal this AMF will serve as backup; Region ID and Set ID of AMF is provided; TAI List is provided.

If all possible AMF instances or a subset of the AMF instances is used by the CBCF for warning message delivery is subject to operator policy.

Furthermore, the CBCF can use the Nnrf_AccessToken Service from the NRF for OAuth2 authentication of HTTP transport between CBCF and an AMF.

Service Communications Proxy

The Service Communication Proxy (SCP) was introduced in 3GPP Release-16 and includes one or more of the following functionalities. Some or all SCP functionalities may be supported in a SCP single instance:

- Delegated Discovery
- Message forwarding and routing to destination NF/NF service.
- Message forwarding and routing to a next hop SCP.
- Communication security (e.g., authorization of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc.

Load balancing, monitoring, overload control functionality provided by the SCP is left up to implementation.

More than one SCP can be present in the communication path between NF Services.

The SCP, although not a Network Function instance, can also be deployed distributed, redundant, and scalable. Such a network reliability design shall work in both communication modes, i.e. Direct Communication and Indirect Communication as shown in figure 2. In the Direct Communication mode, the CBCF (NF A) is involved in the reliability related procedures. In Indirect Communication mode, the SCP is involved in the reliability related procedures.

The NF discovery and NF service discovery enable Core Network entities (e.g., CBCF or SCP) to discover a set of NF instance(s) and NF service instance(s) for a specific NF service or an NF type (e.g., AMF).

In order for the CBCF or SCP to obtain information about the AMF and/or AMF service(s) registered or configured in a

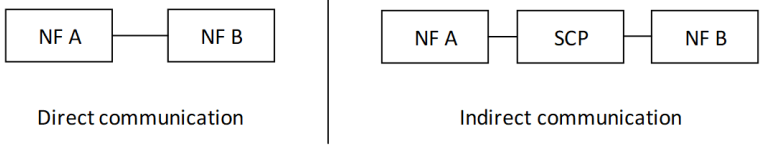


Figure 2: NF/NF service inter communication

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

PLMN, based on local configuration the CBCF or SCP may initiate a discovery procedure with the NRF by providing the type of the NF and optionally a list of the specific service(s) it is attempting to discover. The AMF may also provide AMF Set related information to enable reselection of AMF instances within the AMF Set.

In the case of Indirect Communication, a CBCF employs an SCP which routes the request to the intended target of the request.

If the CBCF is configured to delegate discovery, the CBCF may omit the discovery procedure with the NRF and instead delegate the discovery to the SCP; the SCP will then act on behalf of the CBCF. In this case, the CBCF adds any necessary discovery and selection parameters to the request in order for the SCP to be able to do discovery and associated selection. The SCP may interact with the NRF to perform discovery and obtain discovery result. However, this applies only to requests and not to the management of subscriptions as described below.

The NRF provides a list of AMF instances and AMF service instances relevant for the discovery criteria. The NRF may provide the IP address or the FQDN of AMF instance(s) and/or the Endpoint Address(es) of relevant AMF service instance(s) to the CBCF or SCP. The NRF may also provide AMF Set ID and/or AMF Service Set ID to the CBCF or SCP. The response contains a validity period during which the discovery result is considered valid and can be cached.

In the case of Direct Communication, the CBCF uses the discovery result to select AMF instance and a AMF service instance that is able to provide a requested AMF Service.

In the case of Indirect Communication without Delegated Discovery, the CBCF uses the discovery result to select a AMF instance while the associated AMF service instance selection may be done by the CBCF, or by an SCP on behalf of the CBCF.

In both the cases above, the CBCF may use the information from a valid cached discovery result for subsequent selections (i.e., the CBCF does not need to trigger a new AMF discovery procedure to perform the selection).

In the case of Indirect Communication with Delegated Discovery, the SCP will discover and select a suitable AMF instance and AMF service instance based on discovery and selection parameters provided by the CBCF and optional interaction with the NRF. The NRF to be used may be provided by the CBCF as part of the discovery parameters. The SCP may use the information from a valid cached discovery result for subsequent selections (i.e., the SCP does not need to trigger a new AMF discovery procedure to perform the selection).

In a given PLMN, Direct Communication, Indirect Communication, or both may apply.

For both Direct Communication mode and Indirect Communication mode, the CBCF may subscribe to status change notifications of AMF instance from the NRF. If the CBCF is notified by the NRF or detects by itself (e.g., request is not responded) that the AMF instance is not available anymore, another available AMF instance within the same AMF Set is selected by the CBCF in Direct Communication mode.

For Indirect Communication mode, the SCP and CBCF may subscribe to status change notifications of AMF instances from the NRF.

When multiple AMF instances within an AMF Set are exposed to the CBCF or SCP and the failure of an AMF instance is detected or notified by the NRF, i.e. it is not available anymore, the CBCF or SCP selects another AMF instance of the same AMF Set.

Warning message delivery with SCP

The CBCF uses the services of an SCP to route the request to an AMF instance in the AMF Set that serves the Tracking Areas where the warning message needs to be delivered or where ongoing broadcast needs to be cancelled. The CBCF addresses an AMF Set and the SCP selects an AMF instance in that AMF Set.

The possible communication models with and without delegated discovery are described in the Annex.

Regarding subscriptions to notifications, the CBCF manages this in the same way as when no SCP is present since the SCP does not manage subscriptions on behalf of the CBCF. However, the SCP does proxy subscription requests.

Notifications are sent by an AMF instance to the CBCF and are proxied by an SCP.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

Conclusion

If the CBCF supports communication model A then the AMF Sets and AMF instances need to be configured in the CBCF, since no discovery via the NRF is used.

If the CBCF supports communication model B then the AMF Sets and AMF instances are discovered by using the NRF discover procedure and do not need to be configured in the CBCF.

If the CBCF supports communication model C then the CBCF uses the services of the SCP for routing requests, but otherwise supports the same capabilities as in model B.

If the CBCF supports communication model D then the CBCF uses the services of the SCP for routing requests, where the SCP does the discovery of AMF instances. However, the CBCF needs to support that same discovery capability for the management of subscriptions and is required to subscribe to notifications of AMF status changes with the NRF.

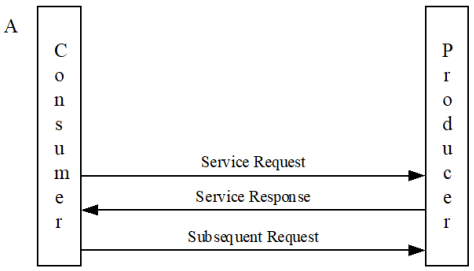
Communication models

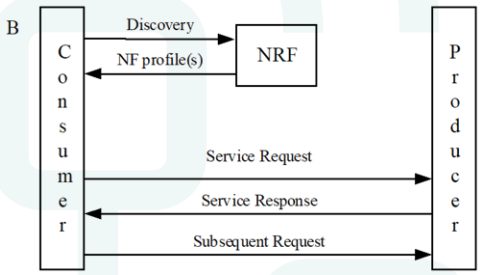
This section provides a high-level description of the different communication models that NF and NF services can use to interact which each other. Table 1 summarizes the communication models, their usage and how they relate to the usage of an SCP.

Table 1: Communication models for CBCF/AMF services interaction summary

Communication between consumer and producer	Service discovery and request routing	Communication model
Direct communication	No NRF or SCP; direct routing	A
Indirect communication	Discovery using NRF services; no SCP; direct routing	B
	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Model A - Direct communication without NRF interaction: Neither NRF nor SCP are used. The CBCF is configured with the "AMF profiles" and directly communicate with an AMF of choice, subject to policy.

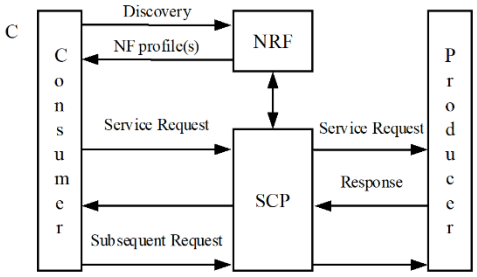


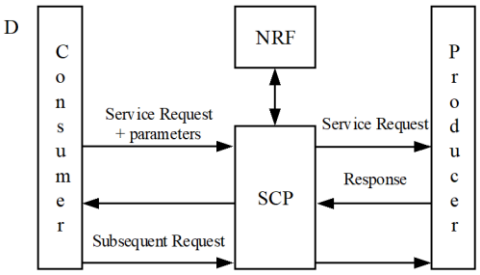


Model B - Direct communication with NRF interaction: CBCF does discovery by querying the NRF. Based on the discovery result, the CBCF does the AMF selection. The CBCF sends the request to the selected AMF instance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

Model C - Indirect communication without delegated discovery: CBCF does discovery by querying the NRF. Based on discovery result, the CBCF does the selection of an AMF Set or a specific AMF instance of AMF set. The CBCF sends the request to the SCP containing the address of the selected AMF pointing to an AMF service instance or a set of AMF Service instances. In the latter case, the SCP selects an AMF Service instance. If possible, the SCP interacts with NRF to get selection parameters such as location, capacity, etc. The SCP routes the request to the selected AMF instance.





Model D - Indirect communication with delegated discovery: CBCF does not do any discovery or selection. The CBCF adds any necessary discovery and selection parameters required to find a suitable AMF for the service request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a suitable AMF instance. The SCP can perform discovery with an NRF and obtain a discovery result.

The communication models apply to routing service requests, but not to subscription management.

Project Coordinator

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Prof. David Gomez-Barquero
Universitat Politecnica de Valencia

iTEAM Research Institute
Camino de Vera s/n
46022 Valencia
Spain

FUDGE-5G Consortium:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242