August 2020

SYSTEM AND METHOD FOR DETECTING INFINITE SIGNALING LOOP IN HIERARCHICAL NRF DEPLOYMENTS

Ravi Shekhar

Ameo Ghosh

Shantanu Bhate

SYSTEM AND METHOD FOR DETECTING INFINITE SIGNALING LOOP IN HIERARCHICAL NRF DEPLOYMENTS

AUTHORS:

Ravi Shekhar
Ameo Ghosh
Shantanu Bhate

ABSTRACT

For larger deployments, where multiple level of Network Function (NF) Repository Functions (NRFs) are deployed, the slightest misconfiguration could lead to an indefinite query loop between NRFs. The indefinite loop in the NRF query would mean repeated timeouts and/or failure of a service discovery request that a consumer had initiated to find a suitable producer. This could lead to signaling failure between a set of consumers and producers, which in turn can lead to Quality of Service (QoS) and Service Level Agreement (SLA) violations. A new Hypertext Transfer Protocol Version 2 (HTTP/2) header, Network Function (NF)-route-record, is proposed, which should be added by an intermediate NRF (relay or proxy) before forwarding any request. The NF-route-record should contain the identity of the peer from which the request was received. The receiving NRF checks the NF-route-record before further forwarding or serving the request. If the NF-route-record matches its own identity, then the receiving NRF would detect the loop. The same can be used in the reverse direction when sending the response from a server (producer) to a client (consumer).

DETAILED DESCRIPTION

The 3GPP 5G standards (23.501, 23.502 and 29.510) introduces the concept of hierarchical Network Function (NF) Repository Functions (NRFs) for large deployments where multiple slices are configured. These NRFs can be deployed at the Public Land Mobile Network (PLMN) Level (configured with whole PLMN information), shared-slice level (configured with information about set of slices) or slice-specific level (configured with information of just a Single-Network Slice Selection Assistance Information (S-

NSSAI) or a slice). These NRFs are the same in terms of features and functionalities but serve different set of Network Functions (NFs) based on configuration. Figure 1 below illustrates an example of NRF hierarchical deployment.

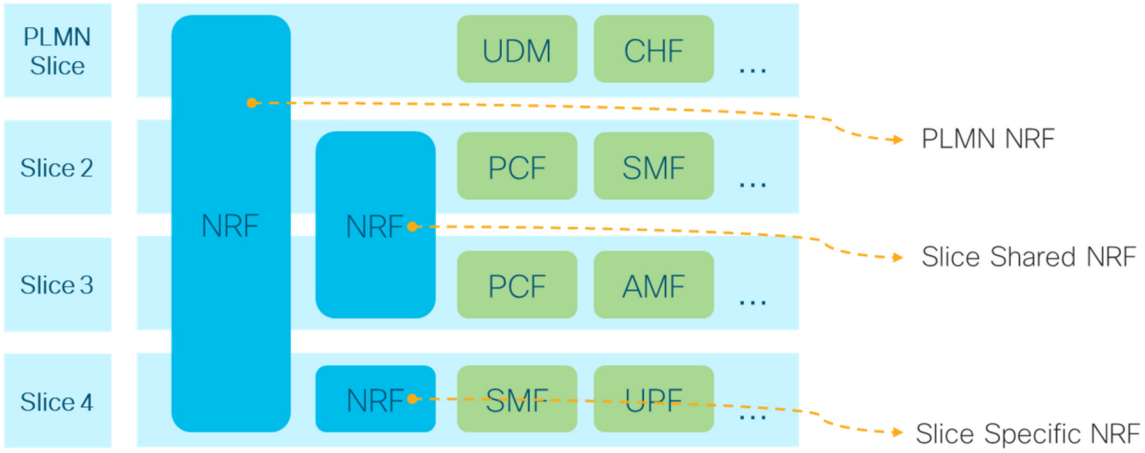

Figure 1-- Hierarchical NRF deployment example

NRFs at different levels communicate with each other for serving services, like a service discovery request or query for an NF-instance. Figure 2 below depicts the 3GPP defined procedure, defined in 3GPP 29.510, for communication between various NRFs at different levels e.g., a PLMN NRF can reach a slice-specific NRF using a shared-slice NRF as an intermediate NRF.

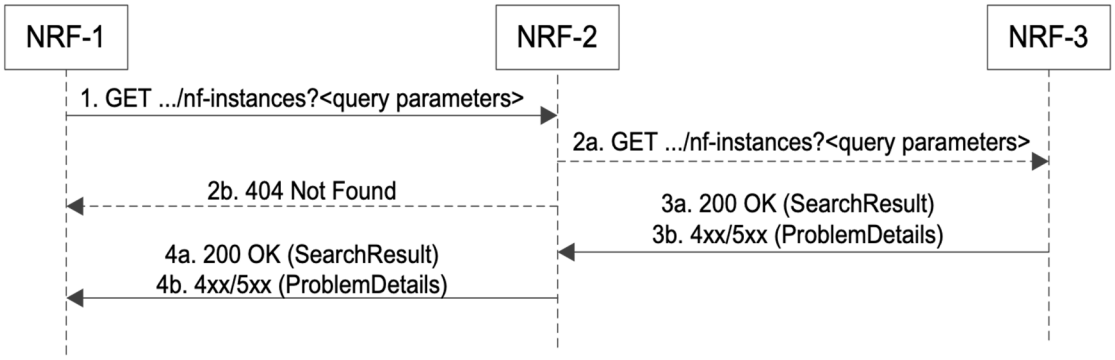

Figure 2 -- NRF communicating using intermediate forwarding NRF

For large deployments the number of NRFs could substantial and they could be geographically distributed. Proper configuration is required for hierarchical NRFs to work through intermediate NRFs. Intermediate NRFs can be configured to work either in a forwarding mode or a redirecting mode. In the forwarding scenario, the NRF that received the request forwards it to another NRF which determines if it can serve the request or needs to forward it further. This mechanism of NRF-to-NRF interaction (in the same PLMN) creates a possibility of an indefinite loop between the NRFs, e.g., due to misconfiguration, as depicted in Figure 3 below. The current 3GPP standards do not have any solution to protect against such indefinite loop.

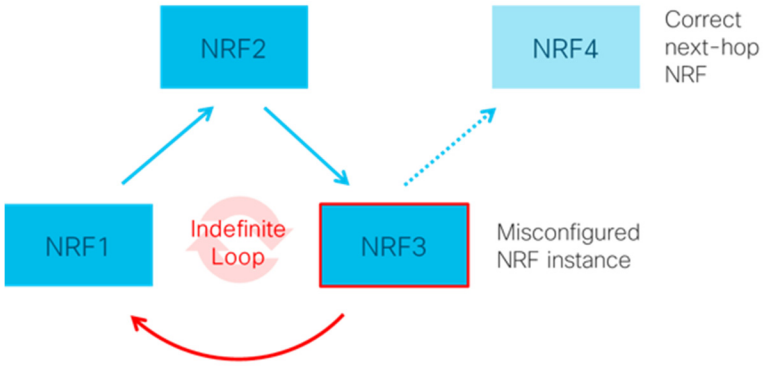

Figure 3 -- Indefinite loop due to misconfiguration in NRF

The indefinite loop in NRF query would mean repeated timeouts and/or failure of a service discovery request that a consumer had initiated to find a suitable producer. This could lead to a signaling failure between a set of consumers and producers, which in turn can lead to Quality of Service (QoS) and Service Level Agreement (SLA) violations leading to revenue loss, especially in case of low latency services.

A new Hypertext Transfer Protocol Version 2 (HTTP/2) header, NF-route-record, is proposed, which should be added by an intermediate NRF (relay or proxy) before forwarding any request. The NF-route-record should contain the identity of the peer from which the request was received. The receiving NRF checks the NF-route-record before further forwarding or serving the request. If the NF-route-record matches its own identity,

then the receiving NRF would detect the loop. The same can be used in the reverse direction when sending the response from a server (producer) to a client (consumer). Figure 4 below depicts an example call flow.

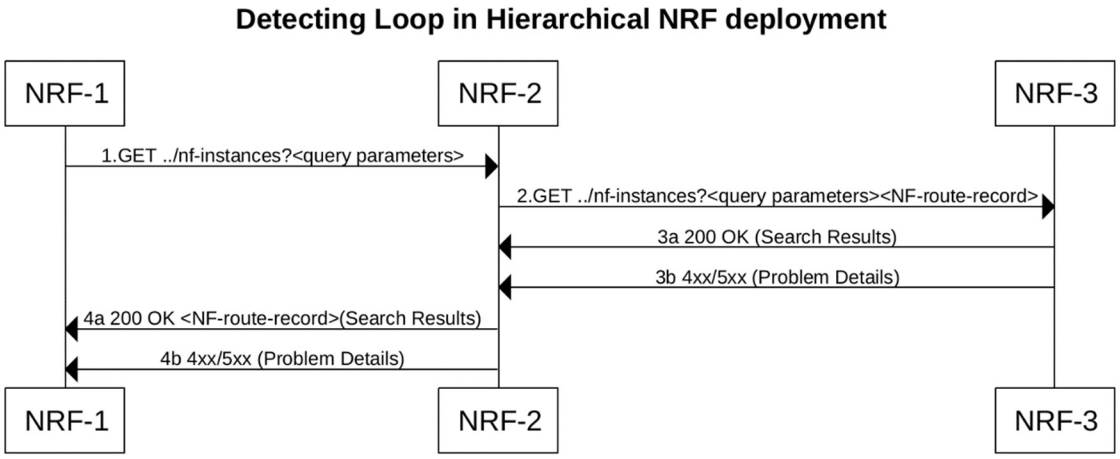

Figure 4 -- Detecting Loop in Hierarchical NRF deployment

The intermediate NRF (relay or proxy agent) checks for forwarding loops when receiving the requests. A loop is detected if the receiving NRF finds its own identity in a NF-route-record header. When such an event occurs, the intermediate NRF answers with the appropriate error code.

The NF-route-record header can also be used for route authorization by a server or a producer to allow (or disallow) the service request coming from a specific client or consumer. For example, a Consumer Internet of Things (CIoT) slice NRF may not allow a Consumer Shared slice NRF to query it for Session Management Function (SMF) instances. In a similar way, the client or consumer may also apply similar authorization rules.

Advantages:

Loop Detection: Using the NF-route-record, the indefinite loop can easily be detected at the receiving NRF and can be reported back to the consumer or client node. This would help in fixing the configuration problem which might have caused the issue. In the interim, the consumer node can be configured to redirect its query to different route.

Route Authorization: The server node (producer which serves the request) can use the NF-route-record for authorizing the session by making sure that the route traversed by the request is acceptable or not before sending the response. The same can be used in reverse direction by client node (consumer) to accept the request based on where the response originates.

In summary, for larger deployments, where multiple level of NRFs are deployed, the slightest misconfiguration could lead to an indefinite query loop between NRFs. The indefinite loop in the NRF query would mean repeated timeouts and/or failure of a service discovery request that a consumer had initiated to find a suitable producer. This could lead to signaling failure between a set of consumers and producers, which in turn can lead to QoS and SLA violations. The new Hypertext Transfer Protocol Version 2 (HTTP/2) header, NF-route-record is provided that is added by an intermediate NRF (relay or proxy) before forwarding any request. The NF-route-record contains the identity of the peer from which the request was received. The receiving NRF checks the NF-route-record before further forwarding or serving the request. If the NF-route-record matches its own identity, then the receiving NRF would detect the loop. The same can be used in the reverse direction when sending the response from a server (producer) to a client (consumer).