# Oracle® Communications

# Network Analytics Data Director Outbound Interface Specification Guide

F83395-02
December 2023

Oracle Communications Network Analytics Data Director Outbound Interface Specification Guide,

F83395-02

# Contents

# My Oracle Support (MOS)

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

# Acronyms

The following table provides information about the acronyms and the terminology used in the document.

**Table Acronyms**

| Acronym | Description |
|---|---|
| 3GPP | 3rd Generation Partnership Project<br>3GPP is the standard body for wireless communications |
| NWDAF | Oracle Communications Networks Data Analytics Function |
| 5G | Fifth Generation<br>5G is the fifth-generation technology standard for broadband cellular networks |
| ACL | Access Control List |
| CNC | Cloud Native Core<br>CNC is a market-leading core network solution utilizing Cloud Native principles and architecture to deliver Service Agility, Innovation, Efficiency, and Adaptability for 4G and 5G network functions including an optional on-premises Cloud Native Environment |
| C-NF | Consumer Network Function |
| CSP | Communication Service Provider |
| HA | High Availability<br>High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime |
| HTTP | Hypertext Transfer Protocol<br>HTTP is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes |
| HTTP2 | Hypertext Transfer Protocol version 2<br>HTTP2 is a major revision of the HTTP network protocol used by the World Wide Web |
| JSON | Java Script Object Notation<br>JSON is a language-independent, text-based data format that can represent objects, arrays, and scalar data |
| mTLS | Mutual Transport Layer Security<br>mTLS authentication ensures that traffic is both secure and trusted in both directions between a client and server. It allows requests that do not log in with an identity provider (like IoT devices) to demonstrate that they can reach a given resource |
| MVP | Minimum Viable Product |
| NF | Network Function |

**Table (Cont.) Acronyms**

| Acronym | Description |
|---|---|
| NRF | Network Repository Function or Network Function Repository Function<br>NRF is a key component of the 5G Service Based Architecture. It maintains an updated repository of all the NFs available in the operator's network along with the services provided by each of the NFs in the 5G core that is expected to be instantiated, scaled, and terminated with minimal to no manual intervention |
| P-NF | Producer Network Function |
| SBI | Service Based Interface<br>SBI is the term given to the API based communication that can take place between two NFs |
| SCP | Service Communication Proxy<br>SCP helps operators to efficiently secure and manage their 5G network by providing routing control, resiliency, and observability to the core network. It leverages IT service mesh (ISTIO) and adds critical capabilities to make it 5G-aware, thereby addressing many of the challenges caused by the new service-based architecture (SBA) in the 5G core |
| SEPP | Security Edge Protection Proxy<br>SEPP as a 5G node is a non-transparent proxy that sits at the perimeter of the Public Land Mobile Network (PLMN) network and enables secured communication between inter-PLMN network messages. It is a Cloud native solution based on microservice architecture which acts as a non-transparent proxy sitting at the perimeter of the PLMN network enabling secured inter NF communication across PLMN networks |
| TCP | Transmission Control Protocol<br>TCP is a connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner |
| TLS | Transport Layer Security<br>TLS and its now-deprecated predecessor, Secure Sockets Layer, are cryptographic protocols designed to provide communications security over a computer network |

# What's New in This Guide

This section introduces the documentation updates for Release *23.3.x* in *Oracle Communications Network Analytics Data Director Outbound Interface Specification Guide*.

**Release 23.3.0.0.1 - F83395-02, December 2023**

There are no updates to this document in this release.

**Release 23.3.0 - F83395-01, September 2023**

- Updated Data Director Message Format with the details of "Kafka Consumer Egress Feed Message Format".

# 1 Introduction

This document provides information on the Data Director Outbound Interface specifications required by customers to use Oracle's SBI Application-Level Traffic Feed solution.

## 1.1 Overview

5G SBI Application-Level Traffic Feed Solution is a common pre-integrated, on demand, and automated solution that is applicable across all NFs, independent of the underlying infrastructure to mirror the 5G SBI message flows towards analytics or third-party tools.

The solution has no specific dependencies, but it provides clear insights into direct NF-to-NF communications. In addition, it maintains security while mirroring the required data and provides all necessary data through standardized interfaces to third-party consumers.

## 1.2 References

For more information on OCNADD, refer to the following documents:

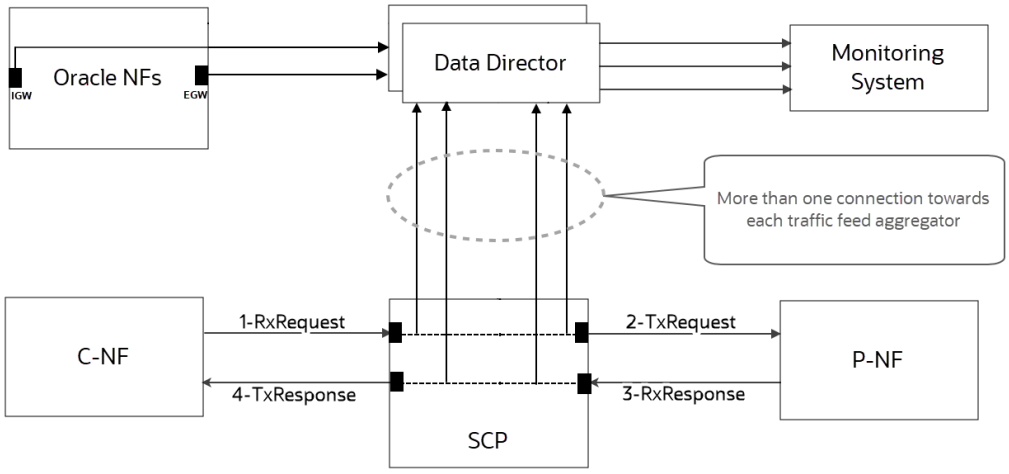
- *Oracle Communications Network Analytics Data Director User Guide*
- *Oracle Communications Network Analytics Data Director Troubleshooting Guide*
- *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core cnDBTier Installation,Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Network Analytics Suite Security Guide*
- *Oracle Communications Network Analytics Data Director Benchmarking Guide*

# 2
# Architecture

This chapter covers the Oracle's 5G SBI Application-Level Traffic Feed solution that demonstrates SBI traffic feed going from Oracle 5G NFs to Oracle Data Director (acting as a traffic feed aggregator).

Following is a high-level block diagram showing the traffic feed from Oracle NFs:

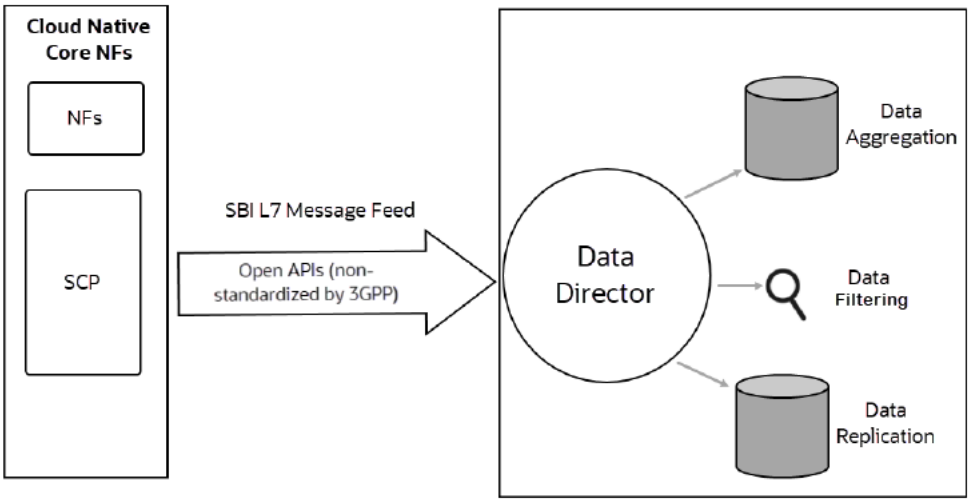
**Figure 2-1 Traffic Feed from Oracle NFs**




The message mirroring takes place through four endpoints covering RxRequest, TxRequest, RxResponse, and TxResponse with respect to SCP and through two endpoints. namely, Ingress and Egress Gateways with respect to Oracle NFs. All transactions are mirrored for both SCP and Oracle NFs.

Following is a high-level block diagram depicting the solution overview:

**Figure 2-2 Solution Overview**




Data Director is a solution within the Network Analytics suite, which addresses the 5G traffic feed aggregation and data enrichment. It assimilates the data required to statistical prediction.

Data Director provides the following key features:

- Aggregation
  - Collects and aggregates the network traffic from multiple NFs, for example, SCP, SEPP, and NRF.
  - Provides the aggregated traffic feed to one or many third-party monitoring tools.
- Filtering
  - Filtering is supported for selected metadata and header attributes in OCNADD release 23.3.0.
  - Delivers only relevant traffic, such as traffic matching specific consumer-id and/or service-name, to the third party tool.
    For more information, see "Data Filtering" and "Data Filters List" sections in *Oracle Communications Network Analytics Data Director User Guide*.
- Replication
  - Feeds multiple third-party systems with the collected feed, for example, to the monitoring, troubleshooting, and security tool.
- Secure Transport (TLS)
  - Provides the data delivery to third-party tools securely.
- High Availability

Data Director is implemented as a Kubernetes service. Multiple Kafka connections from NFs and Data Director will be established to stream the ingress data from NFs. Each instance of the Data Director will support two HTTP2 endpoints of the third-party monitoring tools. The number of connections will depend on the amount of throughput required.

# 3
# Data Director Configuration

This chapter lists the Data Director Configuration requirements on Oracle Communications Cloud Native Environment.

## 3.1 Requirements

Before you begin with the procedure for setting up Data Director in Cloud Native Core, ensure that the following requirements are met:

- The metadata from NFs
- The third-party target that receives the packets
- Optional TLS config
- The HTTP standards require a response for every message sent. Oracle will provide a configuration option to ignore the response.
- The message acquisition point is configurable (**ingress or egreess, or both**) at the NF level

> **Note**
>
> With the HTTP2 ignore the response option enabled the OCNADD considers message transfer as successful as soon as data is sent to 3rd party monitoring consumers. OCNADD does not wait for 200 OK response to consider the message transfer as successful. Message retransmission is not attempted. However, for maintaining the connection status to 3rd party monitoring App endpoints, OCNADD still expects response for each post request sent to 3rd party monitoring App.

## 3.2 Outbound Protocols

Data Director currently supports three Egress Feed types, over which the 5G SBI messages and metadata added by the NFs are forwarded to third-party consumers:

- **HTTP2 Feed:** The HTTP2 Feed is used for monitoring purposes. It employs the HTTP/2 protocol, utilizing JSON as the application layer serialization protocol. Additionally, there is an option to implement TLS for security protection at the transport layer.
- **Synthetic Feed:** The Synthetic Feed operates through a TCP connection, enabling the transmission of synthetic packets. These packets contain comprehensive L2 to L7 information, complete with synthesized layers and necessary information. For added security at the transport layer, optional TLS is available.
- **Kafka Consumer Feed:** The Kafka Consumer Feed allows 3rd-party consumers to retrieve the 5G SBI messages and metadata introduced by the NFs in the form of JSON documents, using the Kafka consumer API. To enhance security during transmission, TLS is employed at the transport layer.

## 3.2.1 Metadata

The following table lists the components that are part of the available metadata from SCP:

> **Note**
>
> For more information on each metadata component, see Data Stream Contents.

**Table 3-1 Format based on 3GPP**

| Metadata | Information |
|---|---|
| correlation-id | This is a unique identifier in the message for correlation within a single transaction.<br>• If an intermediate Oracle NF like SCP or SEPP sees a correlation-id custom header in the message, then it forwards the header without any modification.<br>• Oracle NFs add the correlation-id custom header in the responses. |
| consumer-id | This is a 5G NF Instance ID of the NF originating the received message.<br>• Depends on the presence of the User-Agent header in the received service request<br>• Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN> |
| producer-id | This is a 5G NF Instance ID of the destination NF.<br>• Oracle SCP can find the destination NF instance Id using the authority in the service request and learning from the NRF.<br>• Other Oracle NFs may not be able to find NF instance id of destination in be able to put destination FQDN |
| consumer-fqdn | This is a FQDN of the network function originating the received message.<br>• Depends on the presence of User-Agent header in the received service request<br>• Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN> |
| producer-fqdn | This is an FQDN of the destination NF. It depends on the presence of FQDN in the authority of service request. |
| hop-by-hop-id | Oracle NFs can add Hop-by-Hop id to identify a request and response pair to the next node. This is required in addition to correlation-id for uniquely identifying the request-response pair in case of re-routing. |

**Table 3-1 (Cont.) Format based on 3GPP**

| Metadata | Information |
|---|---|
| reroute-cause | Indicate the re-route cause. Contains one of the following:<br>• Circuit breaking: Flag to indicate that a message is an alternate attempt due to circuit breaking functionality at the SCP<br>• Outlier detection: Flag to indicate that a message is an alternate attempt due to outlier detection functionality at the SCP<br>• Egress-rate-limit: Flag to indicate that a message is an alternate attempt due to egress rate limiting functionality at the SCP<br>• producer-nf-congestion: Flag to indicate that a message is an alternate attempt due to producer NF congestion<br>• Error received<br>• Timeout<br>• Not Available |
| timestamp | This is a timestamp (in nanoseconds) at the traffic feed trigger point when the message is received or forwarded by the SCP. It is an epoch time. |
| message-direction | This is a parameter to indicate whether a message is ingress to or egress from NF. It can be indicated by putting the traffic feed trigger point name.<br>• RxRequest<br>• TxRequest<br>• RxResponse<br>TxResponse |
| feed-source | Source of this traffic feed. This contains the key-value of different identity of the node sending the traffic feed.<br>• Feed-source :<br>– nf-type = SCP<br>– nf-fqdn = SCP's FQDN<br>– nf-instance-id = SCP's NF instance id<br>– pod-instance-id = SCP-worker's pod instance id |

## 3.2.2 Data Director Message

The 5G SBI message that is received or forwarded contains the following components:

- HTTP2: HTTP2 Headers - All received HTTP2 standard and 3gpp defined headers.
- Received Data Director Message Payload

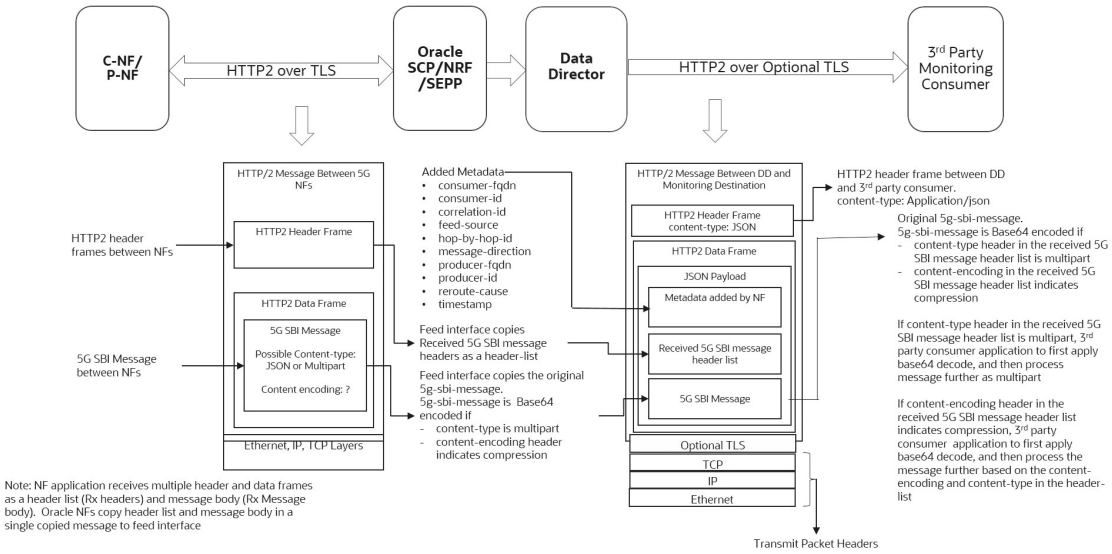
### 3.2.2.1 Data Director Message Format

The Data Director supports the following message formats:

- HTTP2 Message Format
- Synthetic Packet Message Format

- Kafka Consumer Egress Feed Message Format

### HTTP2 Message Format




Data Director supports HTTP2 feed for forwarding from Data Director to third-party monitoring consumer applications. 5G monitoring data is forwarded to third-party monitoring consumer using HTTP2 POST requests. The following components are delivered as JSON payload in the HTTP2 data frames:

- Original received 5G SBI message headers as a header-list.
- Original received 5g sbi data as 5g-sbi-message
- Metadata-list added by NF

The 5g-sbi-message forwarded to third-party consumer application is Base64 encoded if:

- The content-type header in the received 5G SBI message header list is multipart

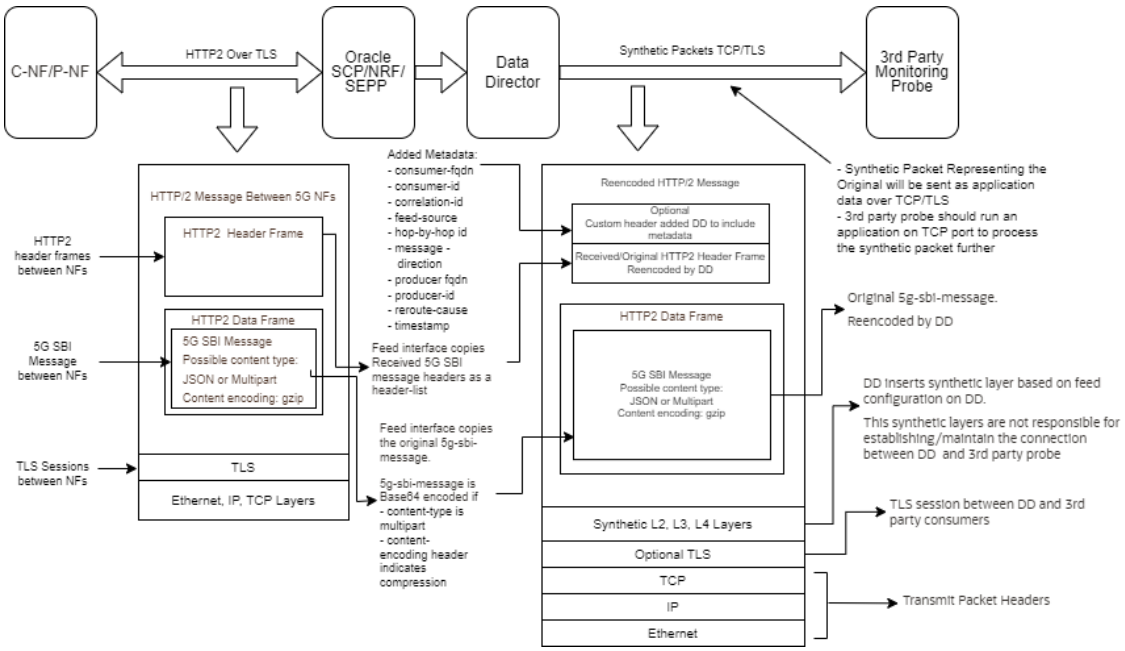
Or

- The content-encoding in the received 5G SBI message header list indicates compression

If the "content-type" header in the received 5G SBI message header list is labeled as "multipart," the third-party consumer application performs an initial base64 decode. Subsequently, the application proceeds to process the message as multipart content.

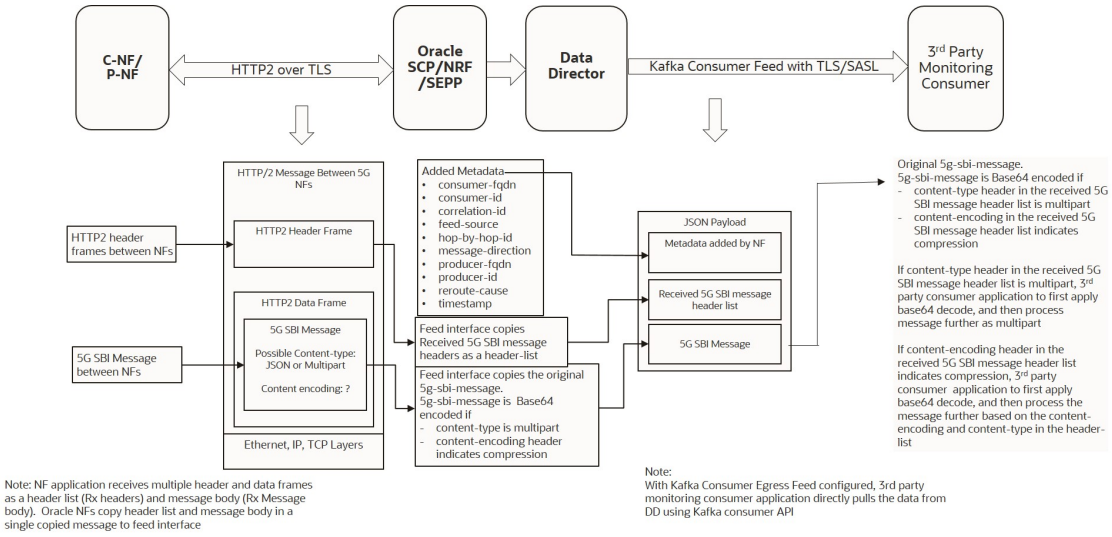
When the "content-encoding" header in the received 5G SBI message header list shows compression, the third-party consumer application first applies base64 decode. Then, it processes the message further based on the content-encoding and content-type in the header list.

### Synthetic Packet Message Format




OCNADD converts incoming JSON data into network transfer wire format and sends the converted packets to the third-party monitoring applications in a secure manner. The third-party probe feeds the synthetic packets to the internal monitoring applications. The feature helps third-party vendors to eliminate the need of creating additional applications to receive JSON data and converting the data into probe compatible format, thereby saving critical compute resources and associated costs.

**Kafka Consumer Egress Feed Message Format**




OCNADD supports the external Kafka consumer applications using the external Kafka Feeds. This enables third-party consumer applications to directly consume data from the Data Director Kafka topic, eliminating the need for any egress adapter.

Clients need to be authenticated through either SASL or SSL (mTLS) for authorization by Kafka. As a result, enabling external Kafka feed support requires specific settings to be activated within the Kafka broker. This ensures mandatory authentication of Kafka clients by the Kafka service.

OCNADD only allows authorized and authenticated third-party applications to use the Data Director Kafka service. Application authorization is handled using the KAFKA ACL (Access Control List) functionality. Access control for the external feed is established during Kafka feed creation. Presently, third-party applications are exclusively allowed to READ from a specific topic using a designated consumer group.

## 3.2.2.2 Third-Party Feed Format

### Third-Party HTTP2 Feed Format

A third-party HTTP2 feed contains the following components:

**Figure 3-1 Third-Party HTTP2 Feed Format**

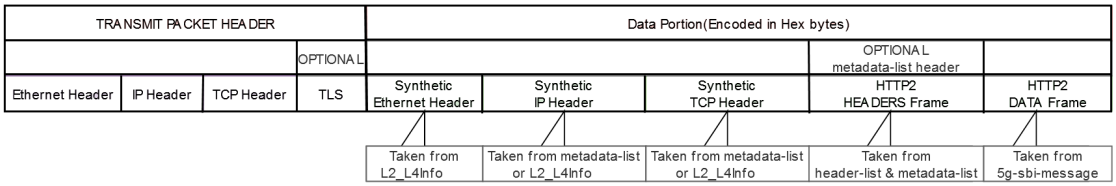
| Transmit Packet Header | | | | Data Portion | | |
|---|---|---|---|---|---|---|
| | | Optional | | JSON | | |
| IPv4 Header | TCP Header | TLS | HTTP/2 Hdr | Mirror 5G SBI Message | Received 5G SBI Message Headers | Metadata Added by Mirror Feed Source |

Following TLS options are supported:

- TLSv1.2 (minimum) with oracle approved TLS Ciphers
- TLSv1.2 with Static Key Cipher support (TLS_RSA_WITH_AES_128_GCM_SHA256)
- No TLS (H2C)

### Third-Party Synthetic Feed Format

A third-party synthetic feed contains the following components:




## 3.2.2.3 Example for the JSON Data

> **Note**
>
> For more information on the metadata list, see Metadata.

Following is an example for the JSON data:


```
{
    "version":"Major.Minor.Patch",
    "metadata-list":{},
    "header-list":{
        ":authority":"10.75.224.64:30065",
        ":method":"PUT",
        ":path":"/USEast/nudm-uecm/v1/imsi-556670000000000/registrations/
amf-3gpp-access",
        ":scheme":"http",
        "content-type":"application/json",
        "3gpp-sbi-target-apiroot":"http://
udm1svc.default.svc.cluster.local:8080/USEast",
        "3gpp-sbi-message-priority":"5",
        "content-length":"501",
        "accept-encoding":"gzip",
        "user-agent":"Go-http-client/2.0"
    },
    "5g-sbi-message":{
        "guami":{
            "plmnId":{
                "mcc":"233",
                "mnc":"23"
            },
            "amfId":"100000"
        },
        "pei":"imei-456565651000000",
        "attrib1":"abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib2":"abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib3":"abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib4":"abcdefghijklmnopqurestuvwxqweoeqwowertyo432123445678",
        "attrib5":"abcdefghijklmnopqurestuvwxqweoeqwowert234yo123445678",
        "pcscfRestorationCallbackUri":"http://pcf1.pcf1svc.svc.cluster.local/
notification/udmtest"
    }
}
```

4

# Third-party Tool Configuration

Customers need to configure respective HTTP2 endpoints of third-party tools in Data Director. The connection status is managed at the TCP stack level.

## 4.1 Multiple IP Addresses

Each instance of the Data Director will support two HTTP2 endpoints of the third-party monitoring tools.

# 5
# Data Stream Contents

**correlation-id**

This is a unique identifier in the message for correlation within a single transaction.

- If an intermediate Oracle NF like SCP or SEPP sees a correlation-id custom header in the message, then it forwards the header without any modification.
- Oracle NFs add the correlation-id custom header in the responses.

The actual correlation-id custom header name is confirmed during the implementation.

**consumer-id**

This is a 5G NF Instance ID of the NF originating the received message.

- Depends on the presence of the User-Agent header in the received service request
- Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN>

**producer-id**

This is a 5G NF Instance ID of the destination NF.

- Oracle SCP can find the destination NF instance Id using the authority in the service request and learning from the NRF.
- Other Oracle NFs may not be able to find NF instance id of destination in be able to put destination FQDN.

**consumer-fqdn**

This is a FQDN of the network function originating the received message.

- Depends on the presence of User-Agent header in the received service request
- Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN>

**producer-fqdn**

This is an FQDN of the destination NF.

Depends on the presence of FQDN in the authority of service request.

**hop-by-hop-id**

Oracle NFs can add Hop-by-Hop id to identify a request and response pair to the next node.

This is required in addition to correlation-id for uniquely identifying the request-response pair in case of re-routing.

**re-route cause**

Indicates the re-route cause. Contains one of the following:

- Circuit breaking: Flag to indicate that a message is an alternate attempt due to circuit breaking functionality at the SCP.
- Outlier detection: Flag to indicate that a message is an alternate attempt due to outlier detection functionality at the SCP.
- Egress-rate-limit: Flag to indicate that a message is an alternate attempt due to egress rate limiting functionality at the SCP.
- producer-nf-congestion: Flag to indicate that a message is an alternate attempt due to producer NF congestion.
- Error received
- Timeout
- Not Available

**timestamp**

This is a timestamp (in nanoseconds) at the traffic feed trigger point when the message is received or forwarded by the SCP. It is an epoch time.

**message-direction**

This is a parameter to indicate whether a message is ingress to or egress from NF.

It can be indicated by putting the traffic feed trigger point name.

- RxRequest
- TxRequest
- RxResponse
- TxResponse

**feed-source**

Source of this traffic feed. This contains the identity of the node sending the traffic feed.

Feed-source:

- FQDN = NF's FQDN
- NF instance id = NF instance id
- Pod instance id = pod instance id

Data Director makes reasonable attempts to deliver packets in the same sequence as received from each pod (SCP Worker pod, NRF, or SEPP API GW pod).

Due to the parallel nature of sending packets across multiple pods within CNE and IP routing, reception in order at the monitoring system cannot be guaranteed. Note that within a single transaction, request and answer follow the same path and processed by the same pod, therefore, there is no need to follow the packet order across multiple pods.

6

# High Availability for Feed

Data Director will support High Availability as per the requirements of customers.

Messages will be available for up to six hours in case of site connectivity issues. Increased redundancy or message caching will require additional resources. Customers will be provided with an option to configure the message caching for up to six hours.

> **Note**
>
> Current Data Director software release assumes underlying data storage provides data redundancy.

In case of recovery after failure, the data streaming will resume from where it got stopped. If the failure duration is more than the retention duration (based on the HA configuration), the streaming will resume from the oldest available data stored in Data Director.

7

# Error Handling

The error handling is maintained by 5G Core NFs. Data Director is an aggregator of 5G Core NF Feed and streams it towards the third-party tools. However, Data Director can create more than one copy of messages, so the message loss is mitigated. Also, Data Director caches the messages for up to six hours and restarts the stream once connectivity is restored with the third-party system.

> **Note**
>
> Current Data Director software release assumes underlying data storage provides data redundancy.