April 2021

ENTERPRISE PRIVATE 5G SELF-HEALING NETWORK

Abhishek Dhammawat

Rajesh I V

Sri Gundavelli

ENTERPRISE PRIVATE 5G SELF-HEALING NETWORK

AUTHORS:
Abhishek Dhammawat
Rajesh I V
Sri Gundavelli

ABSTRACT

With the advent of Internet-of-Things (IoT) devices being utilized in enterprise deployments, industry is heading towards the deployment of Fifth Generation (5G) technologies in enterprise networks with regulators around the globe opening private as well as shared spectrum to facilitate 5G usage. In enterprise private 5G deployments with use-cases such as factory automation, etc. there is need for minimal service disruptions. Additionally, the UE/subscriber session scale will be increased for 5G deployments and the number of applications having critical use-cases with low latency and high bandwidth will also increase. With all these niches and for supporting URLLC use-cases comes the need for radio access network (RAN) and packet core systems to properly function with no service disruption most of the time. Presented herein are techniques to provide a 5G core system (5GC) system as a self-healing network that facilitates network assurance for enterprise private 5G deployments.

DETAILED DESCRIPTION

Typically, in a packet core deployment when a subscriber observes an issue, they will call the service provider and the issue is tracked and resolved. However, such processes can be time consuming and can cause service interruptions. Due to critical applications and use-cases for enterprise private 5G implementations (e.g., factory automation, etc.), there is need for a self-healing network solution in which the network can take remedial action on its own, thereby reducing service downtime. Further, with private 5G solutions deployed in multiple enterprise verticals for handling critical application requirements, a closed loop system for a timely detection, isolation, and remediation of network problems is vital.

This proposal provides a 5GC system as a self-healing network. An enterprise private 5G solution may include the following key components:

1) Packet Core Gateway to facilitate functionality for an Access and Mobility Management Function (AMF), a Session Management Function (SMF), and a User Plane Function (UPF);
2) A RAN (e.g., to provide any combination of a gNodeB (gNB) and/or a disaggregated RAN involving Central Unit (CU), Distributed Unit (DU) and Radio Unit (RU) components;
3) A network management and assurance (management/assurance) entity; and
4) An authentication server (e.g., an Authentication, Authorization, and Accounting (AAA) server, etc.).

However, the above entities typically do not have capabilities to trigger planned tests acting as clients or 5G sensors (devices simulating 5G clients) in order to check the scheduled or on demand network health for various customer use-cases.

Figure 1, below, illustrates an example 5GC system that includes various new components to facilitate self-healing features of this proposal, such as a 5G enterprise agent that is a medium for executing purpose built 5G test simulations at various network vantage points, an enhanced network management and assurance entity with purpose-built new components having the acumen of sensing 5G fault scenarios and baseline deviations to trigger the 5G enterprise agent with the required tests by passing gleaned 5G context, and enhanced packet core functions (AMF/SMF/UPF) and enhanced RAN components (gNB/CU/DU/RU) that can recognize specific issue Key Performance indicators (KPIs) and can communicate context information to the network management and assurance entity for the issues.

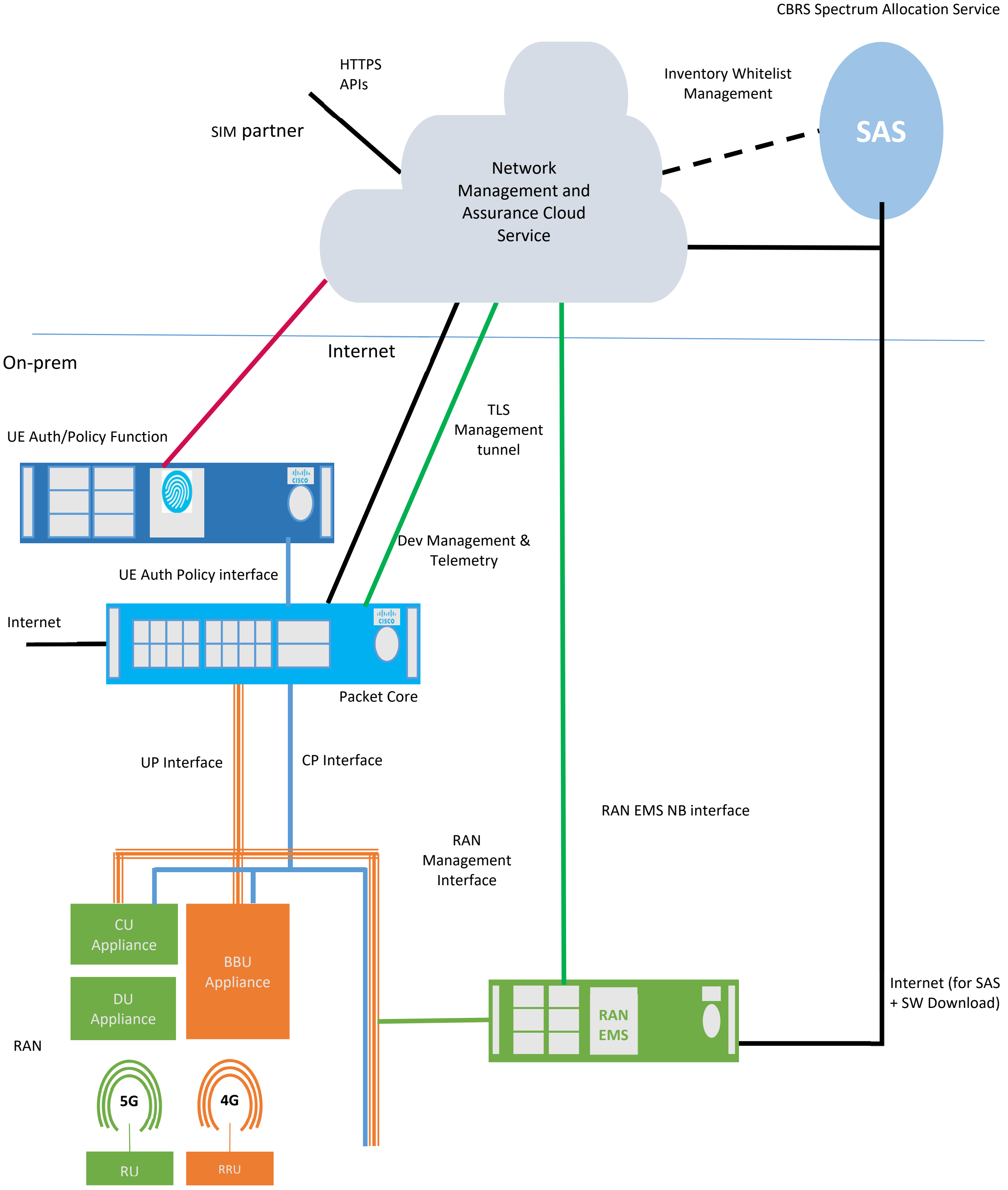


Figure 1: Example 5GC Self-Healing System

A key aspect of this proposal involves a closed-loop between the above-mentioned entities for network assurance in that the packet core gateway events/KPIs can be utilized at the network management/assurance entity to detect anomalies and trigger remedial actions on RAN/packet core elements and/or, in some instances, trigger pre-defined tests to the enterprise 5G agents for better diagnostics.

The 5G agents will have capabilities for running tests on-demand or in scheduled way (based on operator inputs). In various implementations, the 5G agents can be deployed in data centers, branch offices, etc. and can perform various tests acting as clients or gNBs including, but not limited to, registration tests, protocol data unit (PDU) session establishment tests, handover tests, de-registration tests, PDU session release tests, service request procedure tests, and/or dedicated Quality of Service (QoS) flow creation tests.

The agents will interface with the network management/assurance entity for executing purpose built 5G test simulations having the capabilities for running the tests on demand or in scheduled way and also to provide the test reports to the network management entity; thus, the entity will have knowledge about the health of packet core gateway and RAN elements on periodic basis.

The network management/assurance engine can analyze packet core gateway events and KPIs to detect anomalies and trigger appropriate test suites on the network vantage points towards gNB or the packet core gateway as a device under test (DUT) for the underlying issue by passing gleaned 5G context information (e.g., slice, Data Network Name (DNN), application, 5G QoS Identifier (5QI), AMF and functional information, etc.) to gather more intelligence and subsequently trigger the required remedial actions on RAN and/or packet core control-plane (CP) and/or user-plane (UP) functions.

Consider an example workflow, below in Figure 2, that illustrates various example features associated with 5G automatic issue detection and remediation operations that may be performed in the system of Figure 1.

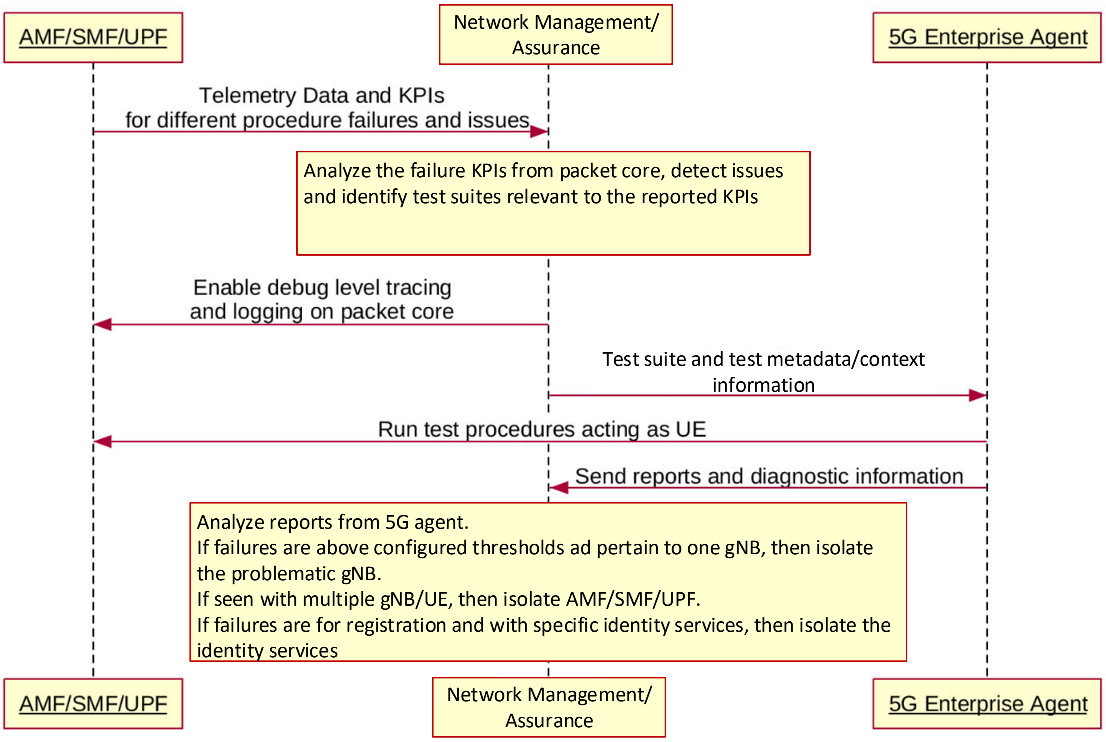

AMF/SMF/UPF
Network Management/ Assurance
5G Enterprise Agent
Telemetry Data and KPIs for different procedure failures and issues
Analyze the failure KPIs from packet core, detect issues and identify test suites relevant to the reported KPIs
Enable debug level tracing and logging on packet core
Test suite and test metadata/context information
Run test procedures acting as UE
Send reports and diagnostic information
Analyze reports from 5G agent.
If failures are above configured thresholds ad pertain to one gNB, then isolate the problematic gNB.
If seen with multiple gNB/UE, then isolate AMF/SMF/UPF.
If failures are for registration and with specific identity services, then isolate the identity services
AMF/SMF/UPF
Network Management/ Assurance
5G Enterprise Agent

Figure 2: Example Workflow

In one instance, 5G enterprise agents can execute pre-defined and/or scheduled test cases in order to report KPIs/test report summaries regarding the health device(s) (e.g., packet core gateway, RAN nodes, etc.) to the network management/assurance entity, which can take action to either move the malfunctioning packet core or RAN elements to a maintenance mode if there are multiple failures or poor KPIs are observed based on the reports. In some instances, the network management/assurance entity can also send alarms to a network operator that may execute further diagnostics for a malfunctioning device in maintenance mode. In still some instances, the network management/assurance entity can detect health issues in a network device and trigger tests corresponding to one or more functionality area(s). Further, the network management/assurance entity can further spawn similar network node(s) to ensure proper functioning/capacity of the network.

Consider, for example, that the network management/assurance entity observes the health of a device and determines an issue such as handover failures based on KPIs provided by the packet core gateway and RAN. In this example, the network management/assurance entity can enable debug logs and packet capturing/monitoring on network device(s) (e.g., packet core gateway and gNB).

Further, the entity can trigger 5G handover tests to be executed via the 5G enterprise agent. Based on reports generated for these tests, the network management/assurance entity can determine if the packet core gateway is having issues and, if similar issues occur with 5G enterprise agent tests, the network management/assurance entity can determine that the issues are not device specific issues but rather packet core gateway or gNB problems.

In another example, if the network management/assurance entity observes handovers failures are occurring for one specific gNB or with multiple gNB, the entity can determine which entity is malfunctioning based on KPIs/reports from enterprise agents and packet core gateway KPIs. For example, if all handover failures occur for a specific gNB, then the problem can be traced to the gNB and, if the problem occurs with multiple gNBs, then the issue can be traced to the packet core gateway and the network management/assurance entity can temporarily move a malfunctioning to a maintenance mode for further diagnostics.

Other use-cases can be envisioned. For example, closed-loop detection techniques as discussed above can be performed for other failures, such as Stream Control Transmission Protocol (SCTP) connection failures, user-plane General Packet Radio Service (GPRS) Tunneling Protocol (GTPu) path management failures between gNBs and a packet core gateway, etc.

The network management/assurance entity may be configured with a new issue processor engine that can maintain a mapping of KPIs received from a network element (e.g., packet core gateway, gNB, etc.) to potential issues and corresponding test suit. Figure 3, below, illustrates an example call flow highlighting an issue processing and remedy framework that can be facilitated via the network management/assurance entity.

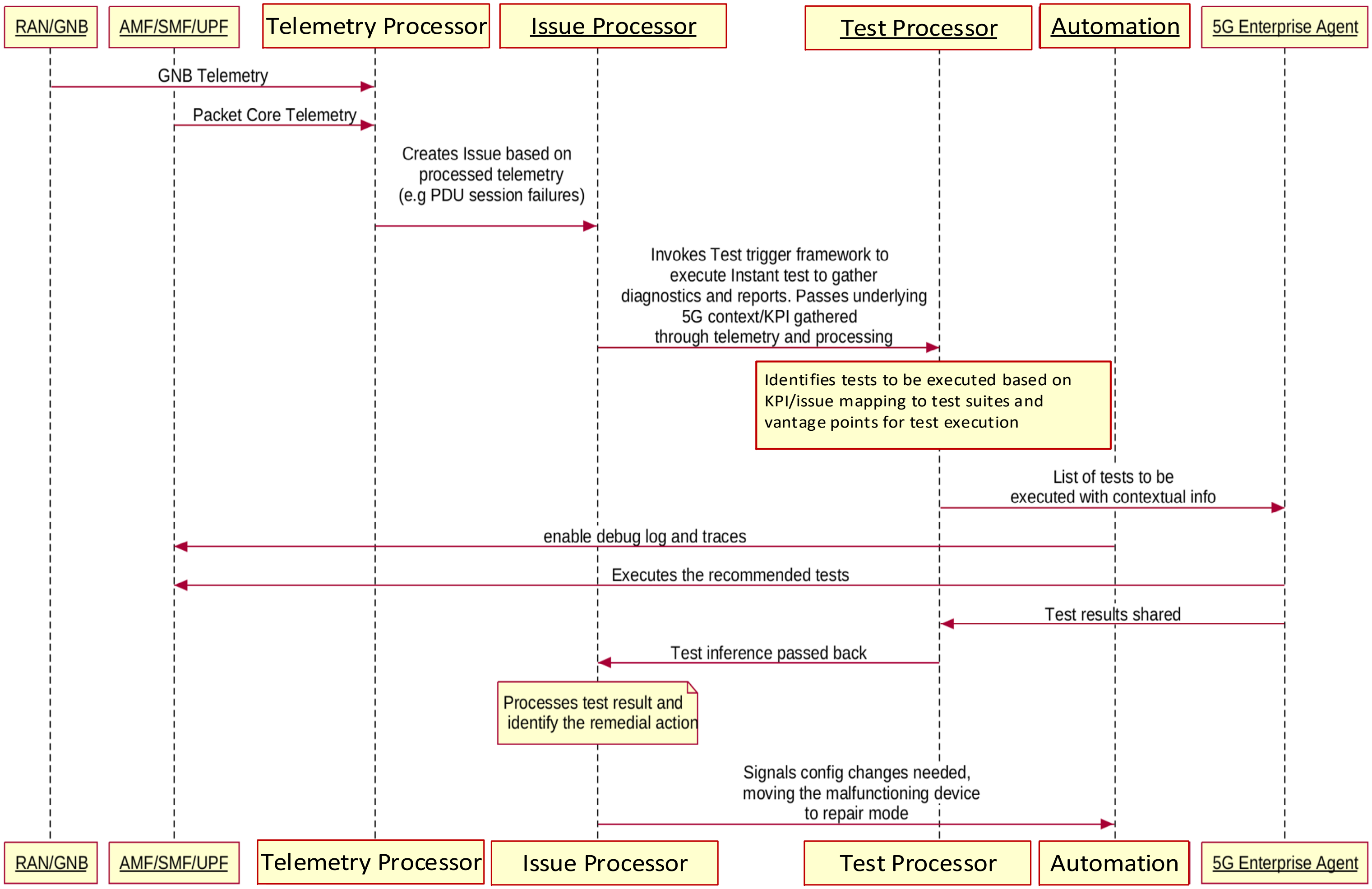

RAN/GNB
AMF/SMF/UPF
Telemetry Processor
Issue Processor
Test Processor
Automation
5G Enterprise Agent
GNB Telemetry
Packet Core Telemetry
Creates Issue based on processed telemetry (e.g PDU session failures)
Invokes Test trigger framework to execute Instant test to gather diagnostics and reports. Passes underlying 5G context/KPI gathered through telemetry and processing
Identifies tests to be executed based on KPI/issue mapping to test suites and vantage points for test execution
List of tests to be executed with contextual info
enable debug log and traces
Executes the recommended tests
Test results shared
Test inference passed back
Processes test result and identify the remedial action
Signals config changes needed, moving the malfunctioning device to repair mode
RAN/GNB
AMF/SMF/UPF
Telemetry Processor
Issue Processor
Test Processor
Automation
5G Enterprise Agent

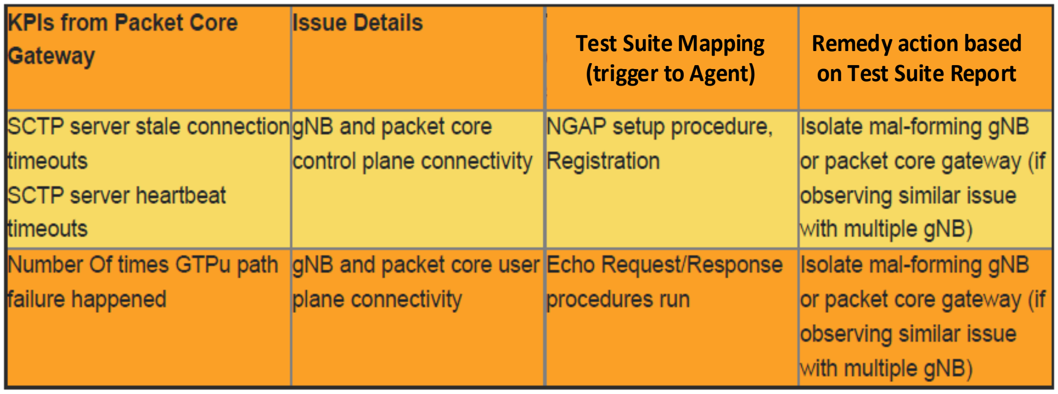
Figure 3: Issue Processing and Remedy Framework

During operation, as illustrated in Figure 3, the network management/assurance entity issue processor engine can analyze the KPIs provided by packet core can perform a lookup on the issue to test suite mapping/database in order to invoke the test engine processor, which can maintain the packet core to 5G enterprise endpoint mapping. The test engine processor can utilize the information regarding test suites and the packet core gateway to select a corresponding 5G enterprise endpoint and issue corresponding tests.

Optionally, the test engine processor can also provide test metadata that can be utilized by a 5G enterprise endpoint during tests. In various instances, test metadata can include DNN information, slice information, application information (e.g., 5QI), policy information, etc.

TABLE 1, below, illustrates different use-cases/KPIs, failures, and test suites that can be initiated for 5G enterprise end point agents by the network management/assurance entity.

TABLE 1: Packet Core Gateway KPIs, Issues, and Test Suite Mapping



KPIs from Packet Core Gateway	Issue Details	Test Suite Mapping (trigger to Agent)	Remedy action based on Test Suite Report
SCTP server stale connection timeouts SCTP server heartbeat timeouts	gNB and packet core control plane connectivity	NGAP setup procedure, Registration	Isolate mal-forming gNB or packet core gateway (if observing similar issue with multiple gNB)
Number Of times GTPu path failure happened	gNB and packet core user plane connectivity	Echo Request/Response procedures run	Isolate mal-forming gNB or packet core gateway (if observing similar issue with multiple gNB)

As illustrates, TABLE 1 identifies per gNB address information (which can include KPIs from the packet core gateway), automated test suite trigger information, and follow-up remedial action information. During operation, the 5G enterprise agents can run the test suites towards gNB/RAN and packet core gateway as a DUT and publish the test reports back to the network management/assurance entity. In some instances, the network management/assurance entity can run logic for remedial action-based report data for different cases, as shown in the matrix for TABLE 1.

Accordingly, the network management/assurance entity can handle test scenarios involving scheduled tests involving baseline deviation checks by collecting KPIs and analyzing the KPIs and also dynamic instant tests based on underlying detected failures.

In one instance, the network management/assurance entity can be configured with threshold values identifying failure percentages for each KPI that are to be satisfied before identifying a potential issue and triggering tests using 5G enterprise agents. In one instance, the network management/assurance entity can use historical data to compare with provided KPIs to determine if potential issues are occurring and to trigger test suits and remedy actions.

The network management/assurance entity can maintain the three levels of assurance data for each packet core, including:

1) Per gNB,
2) Per UE device, and
3) Network device or System level

Consider an example scenario involving SCTP connection failure troubleshooting/assurance. In this example, the AMF can monitor and maintain SCTP connection statistics/KPIs for connectivity between the AMF and the gNB. Such statistics/KPIs may include but not limited to "SCTP server stale connection timeouts" and "SCTP server stale heartbeat timeouts." The AMF provide these KPIs to the network management/assurance entity along with gNB identity and address.

The network management/assurance entity can maintain the issues and corresponding test suite details, such as "NGAP setup procedure and Registration" related cases that can be triggered from 5G Enterprise agent towards the packet core gateway and gNB. The network management/assurance entity can also enable debug level logging and tracing on the packet core.

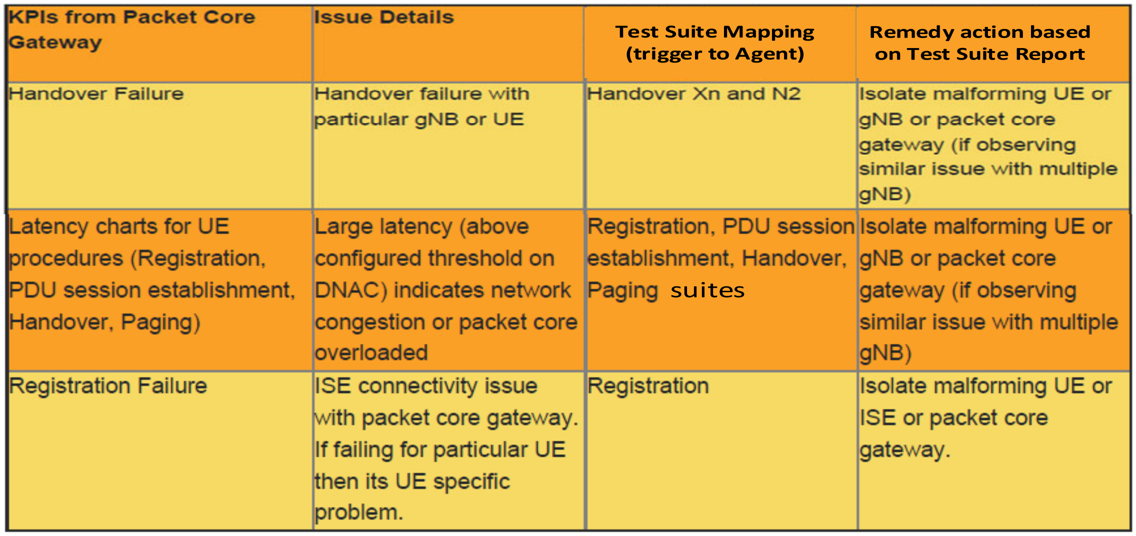
The network management/assurance entity can select a corresponding 5G enterprise agent based on the location of the packet core. The 5G enterprise agent can act as a UE/gNB and connect to the packet core in order to ensure that the packet core does not have any issues with Next Generation Application Protocol (NGAP) setup, registration procedures, and SCTP connection establishment. Thus, the 5G enterprise agent can replicate various scenarios and help to diagnose potential gNB and/or packet core issues such that the 5G enterprise agent can send test reports to the network management/assurance entity, which can determine whether remedial action is to be taken for a particular gNB or packet core in order to isolate a potentially malfunctioning device/node.

Consider another example involving GTPu path failure management. In this example, a UPF can monitor and maintain GTPu management statistics/KPIs for connectivity between the UPF and a gNB. Such statistics can include but not be limited to the number of times GTPu path failure timeouts occur with one gNB and also at the system level. The UPF can provide these KPIs to the network management/assurance entity along with the gNB address and also system level GTPu path management failures.

The network management/assurance entity can then perform analysis using the KPIs to identify issues using the KPI to mapping information in order to trigger a 5G enterprise agent to initiate echo request/response GTP path management messages acting as a gNB towards packet core gateway. The 5G enterprise agent can send test reports to the network management/assurance entity, which can determine whether to take remedial action on the particular gNB or packet core for isolating a potentially malfunctioning device/node.

Consider other examples involving handover failures, registration failures, and/or latency issues in which TABLE 2, below, illustrates various KPI information, issue detail information, test suite mapping, and remedial actions involving such failures/issues.

TABLE 2: Additional Packet Core Gateway KPIs, Issues, and Test Suite Mapping



KPIs from Packet Core Gateway	Issue Details	Test Suite Mapping (trigger to Agent)	Remedy action based on Test Suite Report
Handover Failure	Handover failure with particular gNB or UE	Handover Xn and N2	Isolate malforming UE or gNB or packet core gateway (if observing similar issue with multiple gNB)
Latency charts for UE procedures (Registration, PDU session establishment, Handover, Paging)	Large latency (above configured threshold on DNAC) indicates network congestion or packet core overloaded	Registration, PDU session establishment, Handover, Paging suites	Isolate malforming UE or gNB or packet core gateway (if observing similar issue with multiple gNB)
Registration Failure	ISE connectivity issue with packet core gateway. If failing for particular UE then its UE specific problem.	Registration	Isolate malforming UE or ISE or packet core gateway.

For an example involving potential handover failures, the SMF can maintain KPIs for handover failures and can communicate the KPIs to the network management/assurance entity, which can evaluate the failures in order to identify the involved gNB/packet core gateway nodes. The network management/assurance entity can the check a configured threshold for handover failures. Upon determining that the threshold is exceeded, the entity can determine a corresponding test suite mapping and can notify a 5G enterprise agent to begin an Xn/N2 handover test suite towards the problematic packet core/gNB. The network management/assurance entity can also determine a remedial action to initiate on a particular gNB/packet core for isolating a malfunctioning device/node.

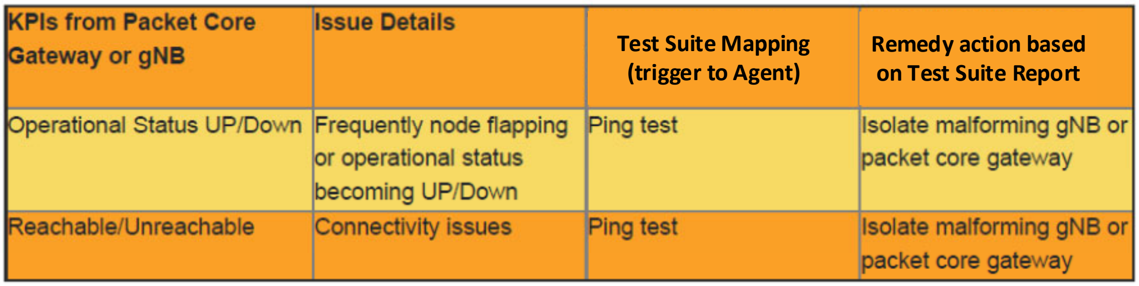
Further, for an example involving registration failures, if registration failures are observed on the AMF, then the AMF can maintain KPIs involving the failures that can be sent to the network management/assurance entity. The network management/assurance entity can identify which identity database and/or packet core are having issues and can utilize the mapping information to identify the registration procedures test suite to be executed. A 5G enterprise agent can then be selected (e.g., based on proximity to the identity database/packet core gateway associated with the registration failures) and triggered to run the tests. After the tests are completed, the 5G enterprise agent sends the test report and results to network management/assurance entity, which can analyze and take remedial actions for isolating the identity database/packet core gateway. In some instances, packet core gateway issues can be detected if the network management entity can detects registration failures involving multiple UEs associated with different identity databases.

In one instance, if handover/registration/PDU session establishment failures are detected for a given UE, then the packet core (e.g., AMF/SMF) can send NAS messages received from the UE to the network management/assurance entity, which the entity can then send to a 5G enterprise agent to replicate the problematic scenario.

Further, for an example involving control plane latency issues, the AMF/SMF can maintain latency information for registration, handover, PDU session establishment procedures. Thresholds can configured on the AMF/SMF for these latencies and if the thresholds are exceeded, KPIs/issues can be reported to the network management/assurance entity, which can identify test suits and trigger a 5G enterprise agent to collect diagnostic information. The 5G enterprise agent can then send back reports and diagnostic information, which can be analyzed to determine if handovers are failing with specific gNB or occurring with many gNBs, which may indicate that malfunctioning devices are packet core gateway nodes (e.g., AMF/SMF).

Finally, TABLE 3, below illustrates additional mapping information for potential issues involving operational status KPIs and reachable/unreachable KPIs that can be reported to the network management/assurance entity.

TABLE 3: Additional Packet Core Gateway KPIs, Issues, and Test Suite Mapping



KPIs from Packet Core Gateway or gNB	Issue Details	Test Suite Mapping (trigger to Agent)	Remedy action based on Test Suite Report
Operational Status UP/Down	Frequently node flapping or operational status becoming UP/Down	Ping test	Isolate malforming gNB or packet core gateway
Reachable/Unreachable	Connectivity issues	Ping test	Isolate malforming gNB or packet core gateway

In summary, techniques of this proposal may provide value for enterprise private 5G deployments in which it is desirable to improve network assurance and minimize downtime of critical applications. Utilizing the techniques described herein, all network entities (e.g., packet core gateway, gNB/RAN, network management/assurance entity, 5G enterprise agents, etc.) can operate in a cohesive and coordinated manner starting from packet core gateway (AMF/SMF/UPF) and RAN KPI/assurance data provisioning can continuing to the network management/assurance entity.

The network management/assurance entity can process assurance data and utilize issue to test suite mapping in order to trigger test suite execution via 5G enterprise agents, which can communicate test reports and diagnostics to the network management/assurance entity. Finally, remedial actions can be provided via the network management/assurance entity in order to isolate malfunctioning network devices and notify a network operator for further diagnostics. Thus, techniques herein may reduce manual network operator intervention and may ease troubleshooting by providing detailed reports, diagnostics, and debug information for problematic scenarios and may also provide remedial actions that can reduce and/or eliminate service interruptions to critical 5G UE/applications.