

P8900S LoadCore – Core Network Solution

Simulation of multiple nodes and interfaces from end-to-end to node isolation for complete Core Network validation.



Testing the 5G Core Network

The deployment of 5G networks is enabling enhanced mobile broadband (eMBB) services with higher data rates, increased capacity, and ultra-low latency. In addition to transforming user experiences, 5G opens new business opportunities through innovations like Network Slicing, Multi-access Edge Computing (MEC), and Private 5G, particularly for sectors such as automotive, manufacturing, energy, and utilities.

These services rely on the robustness and flexibility of the 5G Core (5GC) network. To meet the demands of massive and critical IoT services, service providers must ensure carrier-grade performance across the network. This necessitates thorough testing and continuous validation of 5G Standalone (SA) Core elements in both lab and pre-production environments.

Testing Challenges in 5G Core Networks

The shift to 5G Standalone (SA) Core architecture brings powerful new capabilities but also significant complexity and scale in network testing. Its cloud-native, disaggregated design with many dynamic network functions requires comprehensive, multi-faceted testing to ensure performance, reliability, and security. Key challenges include:

Replicating high-performance production traffic in the lab

Simulating real-world 5G traffic in lab environments is challenging due to 5G's high speed, low latency, and diverse, unpredictable use cases. Poor traffic modeling risks missing critical issues like bottlenecks, traffic distribution inefficiencies, and failures under congestion.

Isolating and testing 5G SA core network functions

The 5G Core's cloud-native, microservices-based design raises the complexity of isolating and testing individual network functions (e.g., AMF, SMF, UPF, PCF).

Ensuring security and resilience

Security testing is complex due to the expanded attack surface from cloud, API, and service-based architectures. Key challenges include simulating advanced attacks (signaling storms, malformed API calls, DDoS), validating mutual TLS and OAuth2 authentication across NFs, and testing resilience against misconfigurations and rogue elements in multi-vendor setups.

Scaling and orchestrating test environments

Continuous integration/delivery demands scalable, automated test environments that can emulate millions of user devices and sessions with varied traffic, dynamically orchestrate NF instances for diverse test scenarios, and integrate with cloud-native monitoring and alerting tools for real-time observability.

Table of Contents

Testing the 5G Core Network 1

Testing Challenges in 5G Core Networks..... 2

P8900S LoadCore – Core Network Solution 4

Key Use Case Examples 5

Flexible Licensing Options 14

Further Resources 15

Related Solutions 15

P8900S LoadCore – Core Network Solution

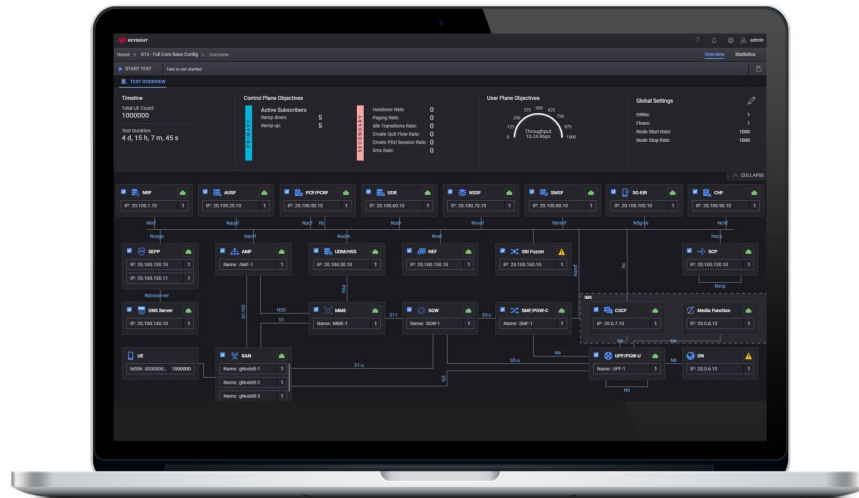


Figure 1. P8900S LoadCore - Core Network Solution

P8900S LoadCore is a SW-only, cloud native solution used to test and simulate multiple nodes and interfaces from end-to-end to node isolation, with real-world subscriber modeling and multi-play traffic generation at scale for complete core network validation.

Key capabilities include:

- Simulate UE behavior in 5G use case deployments: Network slicing, Multi-access Edge Computing (MEC), low latency and offloading, video optimization.
- Perform service validation with subscriber modeling, multiply traffic generation, and Quality of Experience (QoE) measurements.
- Validate complex scenarios for service-based architecture.
- Enforce and validate multiple user-plane QoS characteristics per flow or session.
- Control test traffic mix and intensity using network objectives to independently manage control- and user-planes.
- Scale up to millions of subscribers using stateful application traffic mixes that can interact with real servers and peers.
- Generic licensing scheme offers flexibility to grow with your needs and fit your budget; future-proof and pay-as-you-grow, protecting initial investment.
- Available for deployment on all major public clouds, including AWS Marketplace (both BYOL and PAYG options).

Who benefits from using this solution?

- Mobile Network Operators (MNOs)
- Network Equipment Manufacturers (NEMs)
- Open RAN Component Providers
- System Integrators
- ORAN Open Testing and Integration Centers (OTICs)
- Telecom Research Labs and Academia

Key Use Case Examples

LoadCore provides test solution spanning from early 3GPP feature validation to E2E core network performance testing. Below are the Key use cases highlighted:

- 5G SA use cases
- 4G/5G interworking use cases
- Roaming use cases
- Service Communication Proxy (SCP) testing use cases
- Mobile core testing use cases

5G SA use cases

E2E simulation

LoadCore is optimized to evaluate the scalability and robustness of 5G Core networks under demanding conditions. It provides detailed insight into both Control and User Plane performance, making it ideal for stress testing and advanced procedure validation. Key capabilities include:

- Focus on Control Plane NG-AP (N1/N2) and User Plane (N3) capacity, enabling thorough performance and signaling evaluations.
- Support for thousands of gNBs per VM, allowing large-scale RAN emulation with minimal resource overhead.
- Advanced procedure validation, including scenarios such as Handovers, Paging and Enter/Exit Idle mode.
- Multiple sessions per UE, with support for multiple QoS flows per session to reflect complex traffic patterns.
- Negative testing and impairment injection on SCTP/NGAP, enabling resilience and fault-tolerance verification.

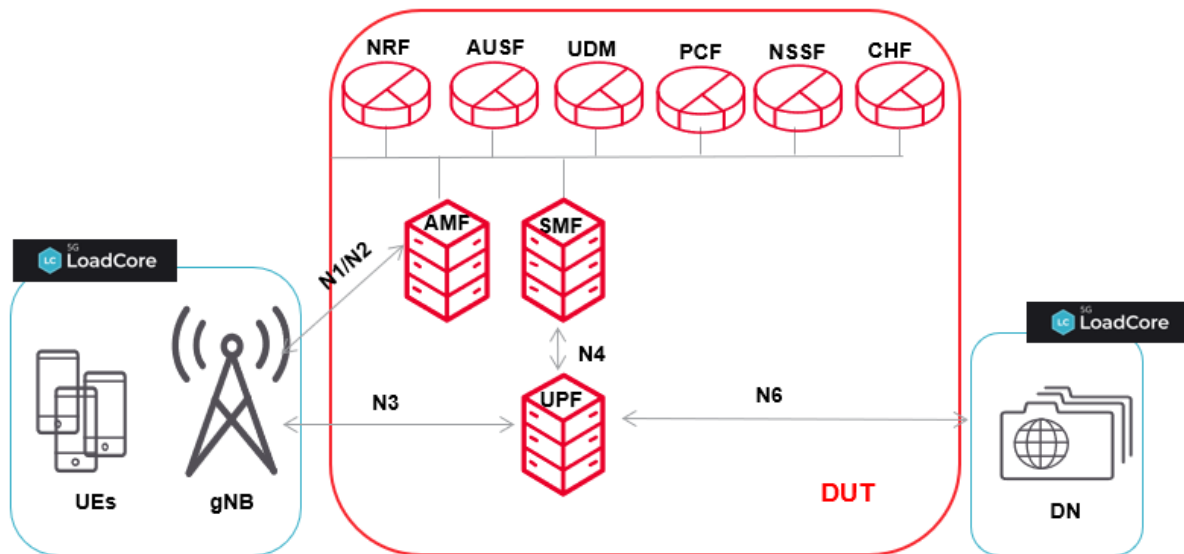


Figure 2. P8900S LoadCore E2E core simulation

AMF or SMF isolation

LoadCore enables focused and high-fidelity testing of the 5G Standalone (SA) Core, specifically targeting AMF and SMF isolation scenarios. Key capabilities include:

- Focused on ControlPlane functional and capacity testing
- AMF and/or SMF validation with SBA wraparound
- Coordinated simulation of N1/N2/N3, Nsmf, Nausf, Nudm, Npcf, Nnrf plus either Nsmf or Namf
- Deploying all nodes as individual entities (i.e. no topology hiding)

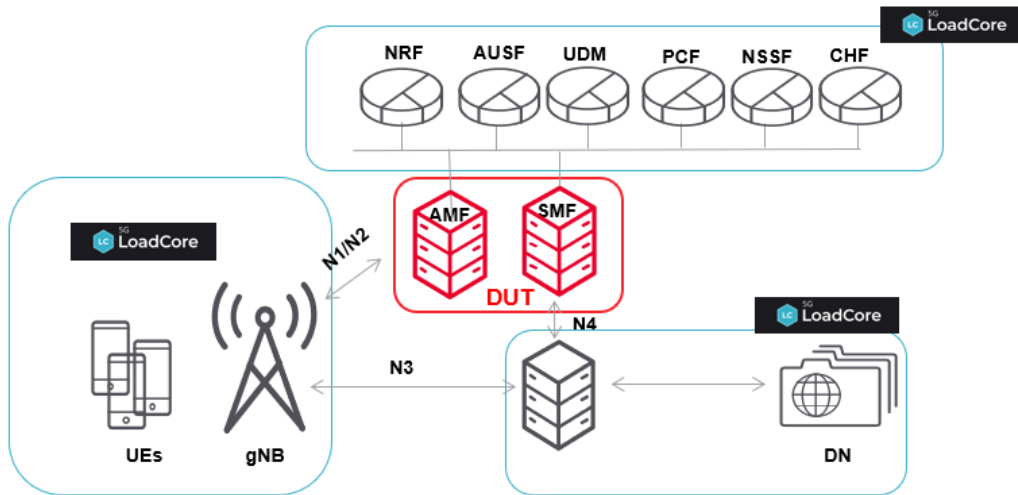


Figure 3. P8900S LoadCore AMF and SMF wraparound

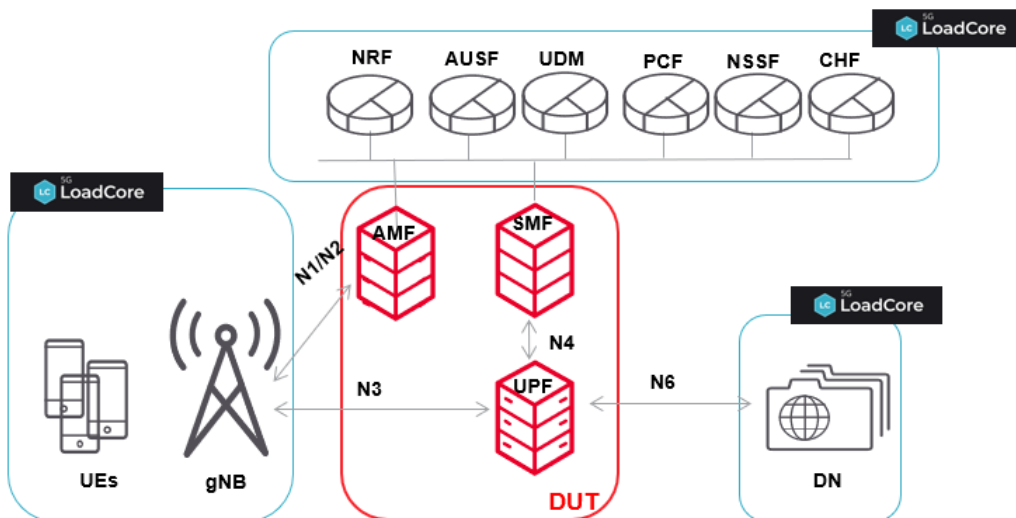


Figure 4. P8900S LoadCore AMF, SMF and UPF wraparound

UPF isolation with N9 & Uplink Classifier

LoadCore delivers advanced capabilities for testing User Plane Function (UPF) behavior and performance in complex 5G network topologies. It enables comprehensive simulation and validation of traffic paths, handovers, and service-based features like MEC and ULCL, making it ideal for both functional and topology-based testing. Key features include:

- Coordinated simulation of interfaces: N3/N4/N9
- Ability to either have both I- and PSA- UPFs under test, or simulate one of them
- MEC validation by testing traffic steering
- Simulation of Handovers between I- and PSA- UPFs
- Support for testing ULCL (Uplink Classifier) topology

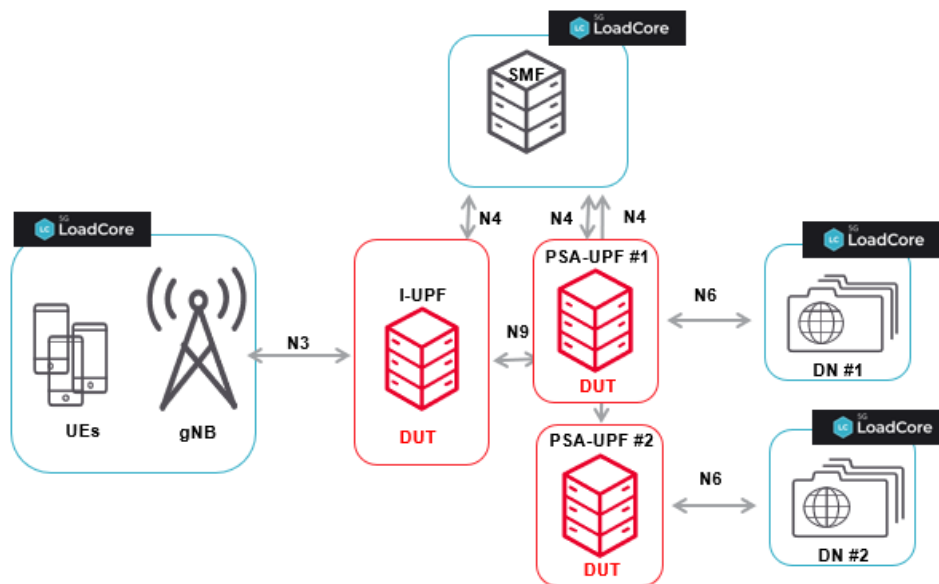


Figure 5. P8900S LoadCore I-UPF and PSA-UPF isolation

SBA nodes isolation

LoadCore provides a robust platform for Service-Based Architecture (SBA) network function testing within the 5G Core, enabling detailed functional and performance validation of individual NFs. Key capabilities include:

- Focused on SBA network function testing, including HTTP/2, HTTPS/2, and OpenAPI compliance.
- Individual validation of key NFs, such as PCF, UDM, AUSF, CHF, and UDR, ensuring conformance and behavior under realistic conditions.
- Performance testing at scale, with support for thousands of concurrent TCP connections toward the Device Under Test (DUT).
- Functional and negative testing using Impairment and Fuzzing, enabling validation under fault, latency, or protocol error scenarios.
- Ability to simulate coordinated HTTP/2 (SBI) and diameter (4G) flows, supporting interworking tests for PCF/PCRF or HSS/AUSF/UDM combinations.

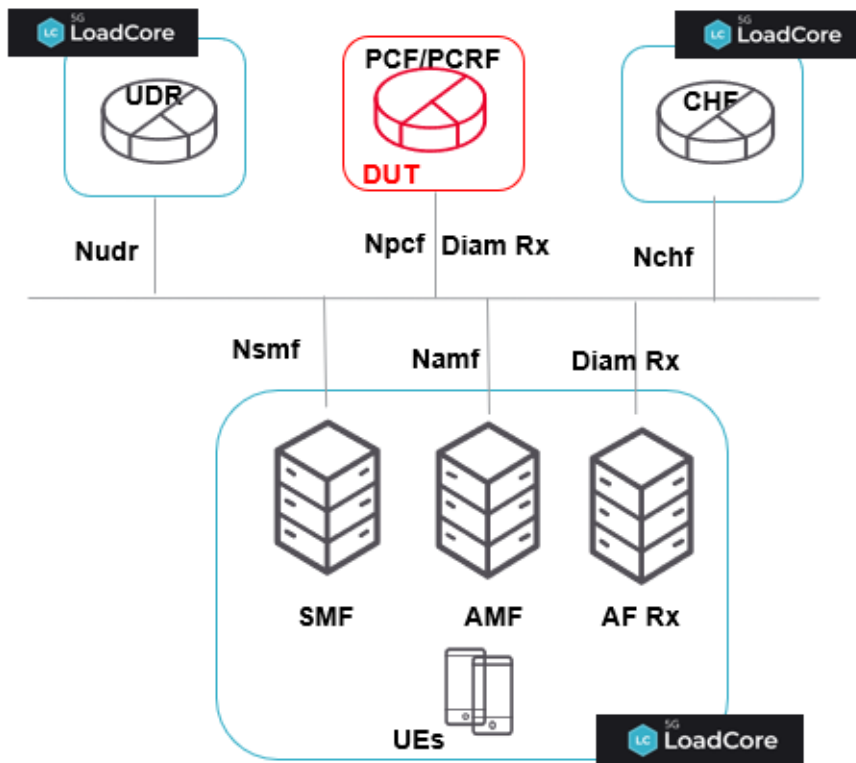


Figure 6. P8900S LoadCore SBA Nodes Isolation

4G / 5G interworking testing

ENB/GNB simulation

LoadCore enables comprehensive testing of interworking scenarios between LTE (4G) and 5G SA/NSA architectures. Key capabilities include:

- Focused on interworking between 4G and 5G
- Coordinated simulation of eNB (S1-MME/S1u) and gNB (N1/N2/N3)
- Scalable RAN simulation, with support for thousands of eNBs and gNBs per VM
- Validate iRAT handovers and EPS fallback

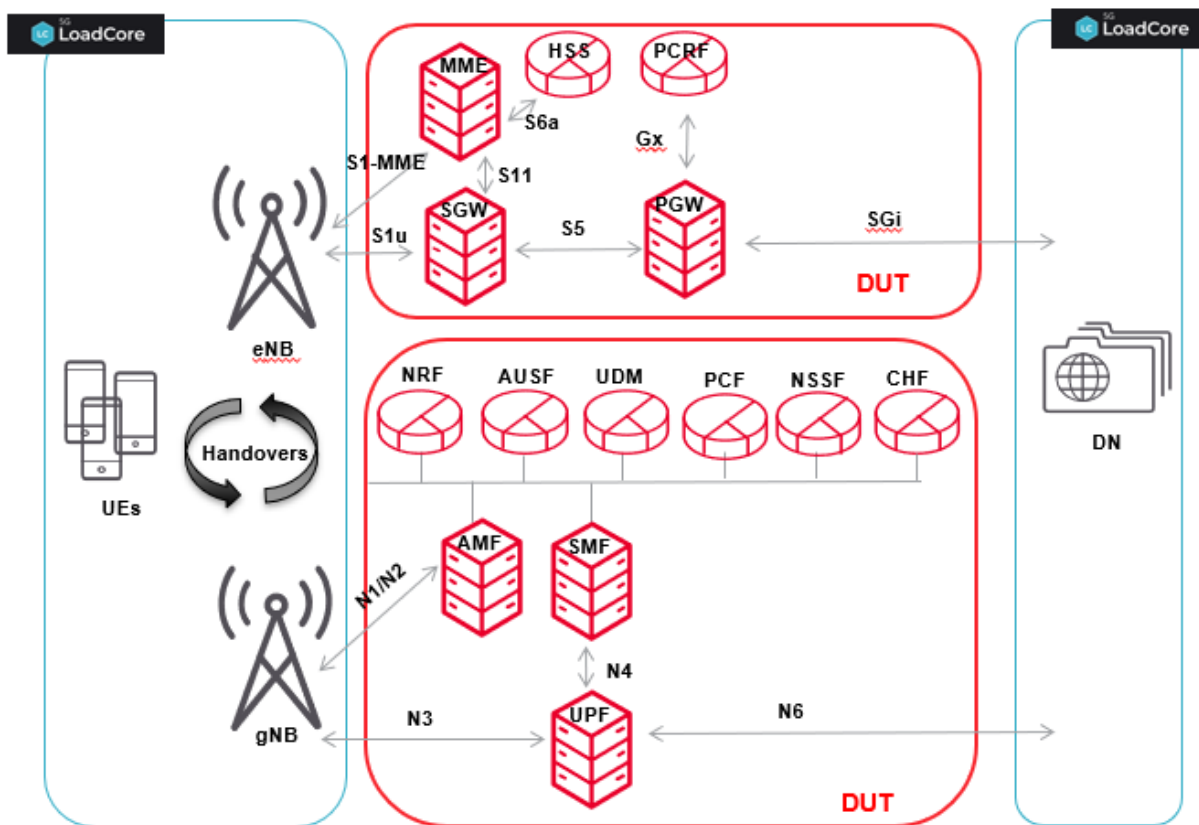


Figure 7. P8900S LoadCore ENG/5G simulation

Roaming use cases

SEPP/N32 testing

LoadCore provides robust capabilities for validating roaming scenarios in 5G SA networks, with a specific focus on SEPP (Security Edge Protection Proxy) and N32 interface testing. This includes simulation of both Home and Visitor SEPP roles and verification of secure, standards-compliant communication between PLMNs. Key features include:

- Support for simulating both Home and Visitor SEPPs over the N32 interface, enabling comprehensive roaming security validation.
- Support for Home Routing topologies, with exposed N16 (SMF interface) and N9 (UPF interface), ensuring end-to-end session continuity across roaming domains.
- Validation of SEPP communication with key components, including:
 - NRF (for NF discovery and registration in roaming scenarios)
 - DNS Server (for domain-based SEPP resolution)
 - Peer SEPP nodes from other PLMNs, including the ability to initiate and manage N32-c connections as required.

SCP testing use cases

Full support for SCP indirect communication

LoadCore offers comprehensive testing capabilities for Service Communication Proxy (SCP) functionality within the 5G Service-Based Architecture (SBA). This includes full validation of Indirect Communication models and custom 3GPP SBI headers, enabling protocol-compliant and highly configurable testing of service routing behavior and discovery mechanisms. Key features include:

- Full support for Indirect Communication models as defined by 3GPP:
 - Model C – Indirect Communication without Delegated Discovery
 - Model D – Indirect Communication with Delegated Discovery
- Complete support for 3GPP-defined custom SBI headers, enabling fine-grained testing of SCP routing logic:
 - 3gpp-Sbi-Target-apiRoot – Specifies the target API root URI when routing requests via SCP.
 - 3gpp-Sbi-Callback – Defines the type of notification expected in asynchronous responses.
 - 3gpp-Sbi-Discovery-<discovery parameter> – Enables delegated discovery using dynamic values like target-nf-type, target-nf-instance-id, and more.

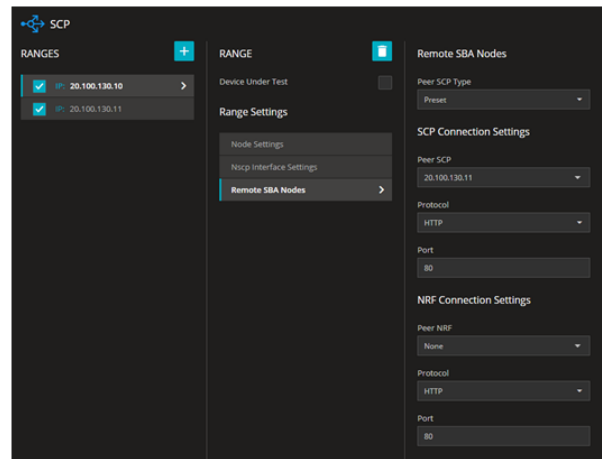
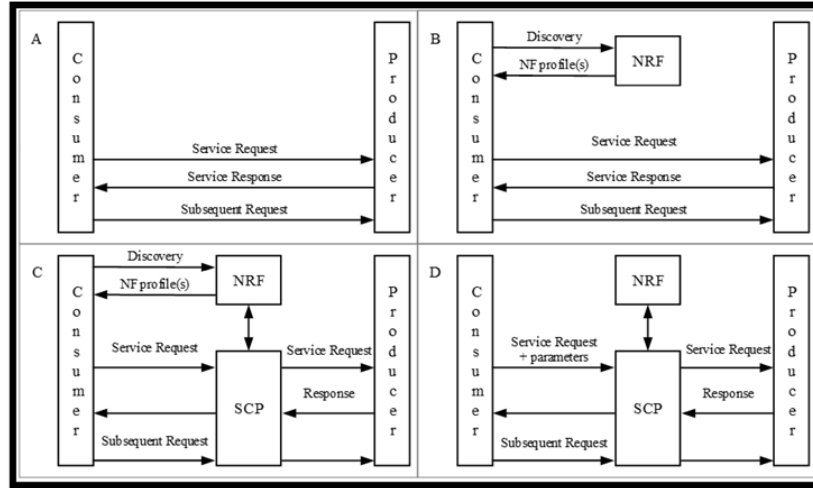


Figure 8. P8900S LoadCore SCP testing

Mobile core testing use cases

Full core simulation

LoadCore offers a comprehensive environment tailored for testing and validating 5G Core network functionalities. With a focus on flexibility, visibility, and performance, it enables users to perform in-depth evaluations of network behavior under realistic conditions. Key features include:

- Ability to deploy and simulate the entire Core, with each Network Function (NF) distinctly activated.
- End-to-end call-coordinated simulation, with all procedures exposed across all interfaces.
- Ideal for probes and network analytics, supporting Control Plane DPI and protocol-level testing.
- Designed for high performance on both the Control and User Planes.

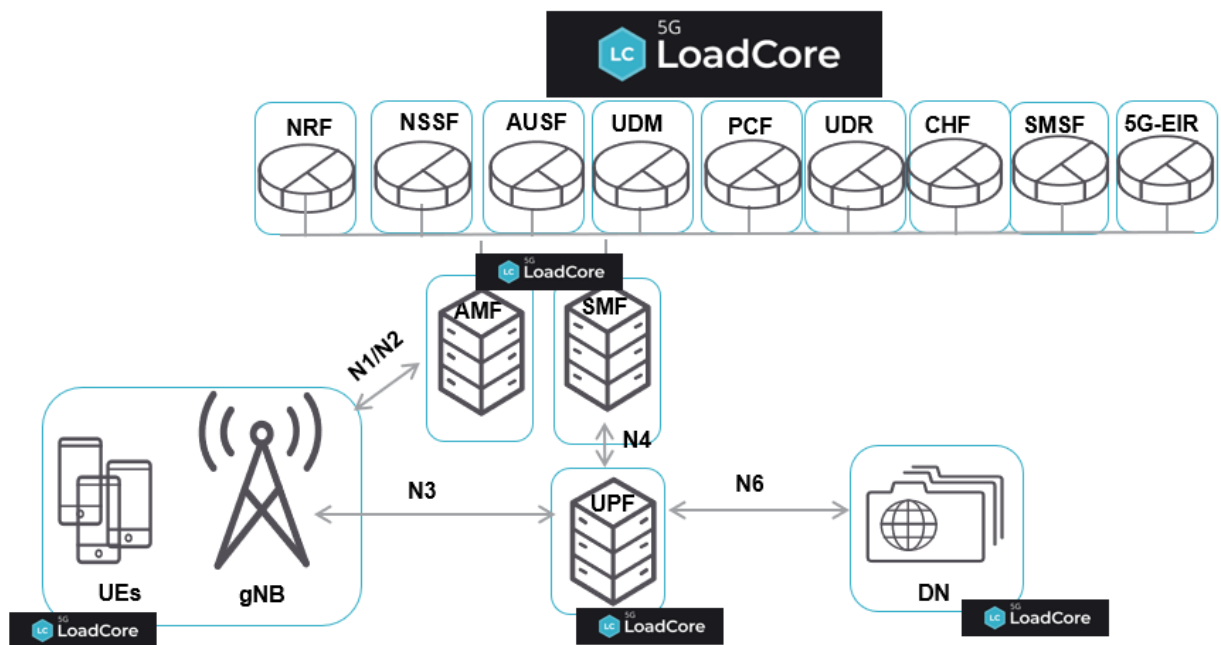


Figure 9. P8900S LoadCore Full Core Simulation

5G SA core security testing

LoadCore enables deep, protocol-aware testing of security procedures and resilience under attack or failure scenarios. Key security testing capabilities include:

- Validation of NAS security procedures, including integrity protection and ciphering for N1/N2 interfaces.
- Authentication and authorization testing via AUSF, UDM, and SEPP, covering both SUPI-based and SUCI-based authentication flows.
- TLS and HTTPS/2 validation for SBA interfaces, ensuring proper encryption, certificate handling, and mutual authentication.
- Negative testing and robustness checks, such as malformed messages, replay attacks, and invalid credentials.
- Testing of SEPP and inter-PLMN roaming security, including end-to-end encryption and trust anchor validation.
- Support for testing security compliance with 3GPP specifications and operator-specific security policies.
- Simulation of attacks and failure scenarios, including DoS, protocol timeouts, and key negotiation failures to validate network resilience.
- UE-generated Malware for validating UPF Deep Packet Inspection (DPI) capabilities and accurate Call Detailed Record (CDR) generation.

Flexible Licensing Options

Keysight offers a wide range of license types and terms to fit your testing needs, allowing cost effective use of assets.

License type	Description
Floating	Networked instruments/computers can access a license from a server one at a time

License Terms	Description
Perpetual	Perpetual licenses can be used indefinitely
Subscription based	Temporary licenses can be used for a limited duration of 6, 12, 24, or 36 months

Further Resources

- [Radio Access and Core Network Test](#)
- [LoadCore-5G-Core-Testing.pdf](#)
- [5G-Core-Testing-with-P8900S-LoadCore-Validating-Performance-and-Reliability.mp4](#)
- [Negative-Testing-using-LoadCore.pdf](#)
- [Webinar/5g-network-slicing--ensuring-successful-implementation-and-valid.html](#)
- [Best Practices for 5G Core Network](#)
- [Nine-Tests-You-Need-Now-for-Edge-to-Cloud-Networking.pdf](#)

Related Solutions

- [P8800S UeSIM RAN Testing Toolset | Keysight](#)
- [P8822S RuSIM RAN Testing Toolset](#)
- [Radio Access and Core Network Test](#)
- [U5040BSCB Open RAN Studio for O-RU Testing and Validation](#)
- [P8850S CoreSIM – Core Simulation RAN Solutions](#)
- [P8827S CuSIM – O-DU Midhaul Solutions](#)
- [P8826S DuSIM – O-CU Midhaul Solutions](#)
- [P8828S RICtest — RAN Intelligent Controller Test Solutions](#)
- [Keysight-Open-RAN-Automated-Compliance-Test-Cases.pdf](#)



Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

This information is subject to change without notice. © Keysight Technologies, 2025, Published in USA, August 7, 2025, 3125-1358.EN