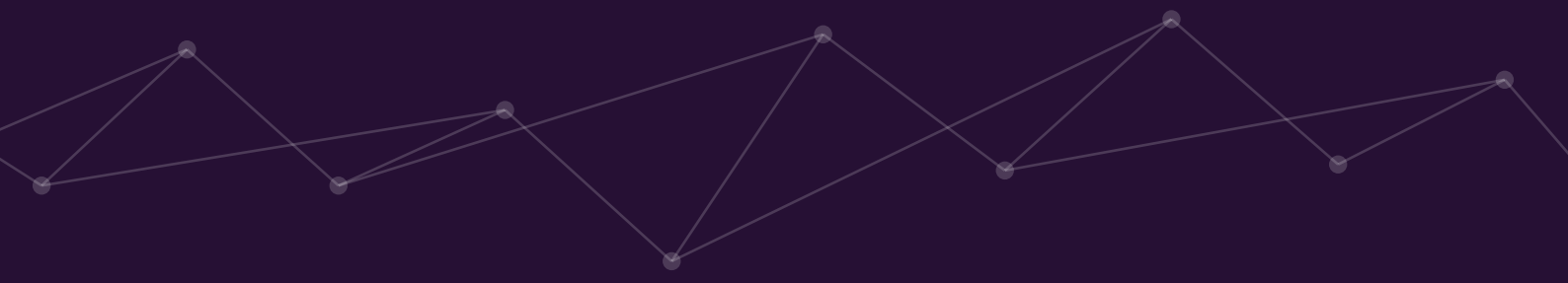
Globberry | Version 2.0 - October 2026



Cloud DRA

DIAMETER ROUTING AGENT



Introduction

This document describes Globberry Cloud DRA, a cloud-ready Diameter Routing Agent designed for routing, mediation, load control and operational visibility across modern telecom signaling environments.

DRA remains a key element in LTE/EPC, IMS, VoLTE/VoWiFi, roaming and 5G NSA environments where Diameter interfaces continue to connect policy, charging, subscriber and application systems. In hybrid 4G/5G networks, it also helps operators simplify legacy Diameter domains while new service-based 5G SA functions are introduced in parallel.

Globberry Cloud DRA is based on a microservice architecture and can be deployed on physical, virtualized or cloud infrastructure. The solution supports horizontal scaling, geo-redundancy, monitoring and flexible integration with existing OSS/BSS and mobile-core environments.

Key functions

- Message relay: route Diameter messages between network components with configurable routing and balancing logic.
- Subscriber-dependent routing: select destination systems according to subscriber identity, profile data, location, segment or service attributes.
- Session binding: keep related messages for the same subscriber or session on the same target component.
- Topology hiding: conceal internal host and realm information from external or partner-facing interfaces.
- Mediation and enrichment: adapt Diameter message attributes and enrich signaling with subscriber or session information.
- Interworking: support integration between Diameter and RADIUS-based domains where required.
- Throttling and protection: limit request rates during peaks and shield downstream systems from overload.

DRA in Modern Telecom Networks

The role of DRA is to reduce the complexity of Diameter signaling by centralizing routing, mediation, load control and topology management. Without a routing layer, adding or replacing a network component can require changes across many directly connected systems.

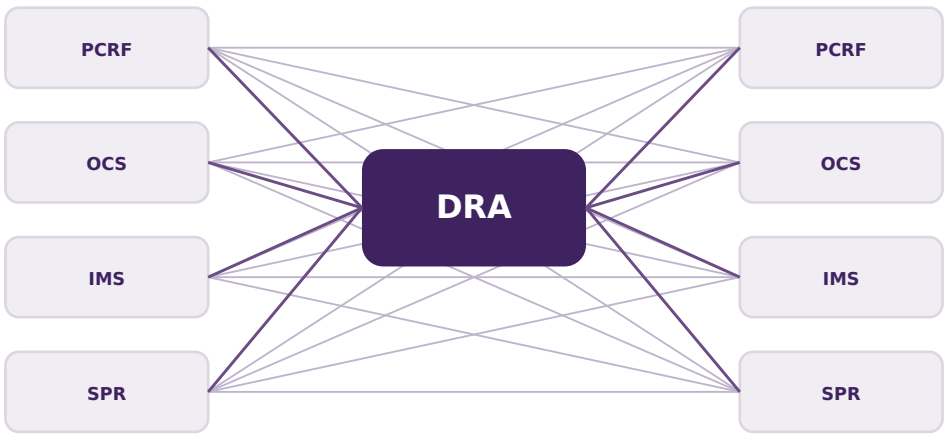
Cloud DRA gives operators a stable signaling hub between mobile-core, policy, charging, subscriber and application systems. Routing rules can be updated centrally, while downstream components can be scaled, replaced or segmented without changing every peer connection in the network.

The DRA is especially useful in environments where multiple vendors, roaming partners, MVNOs, enterprise services, IMS functions and charging systems coexist. It reduces point-to-point Diameter complexity and gives operations teams a single place to manage signaling behavior.

Modern deployment drivers

- Growth of Diameter signaling across LTE/EPC, IMS, VoLTE/VoWiFi and 5G NSA domains.
- Need to protect policy, charging and subscriber systems from signaling bursts and unexpected traffic peaks.
- Coexistence of legacy, virtualized and cloud-native network components from different vendors.
- Need for centralized routing control during migrations, expansions and service launches.

Diameter topology simplification



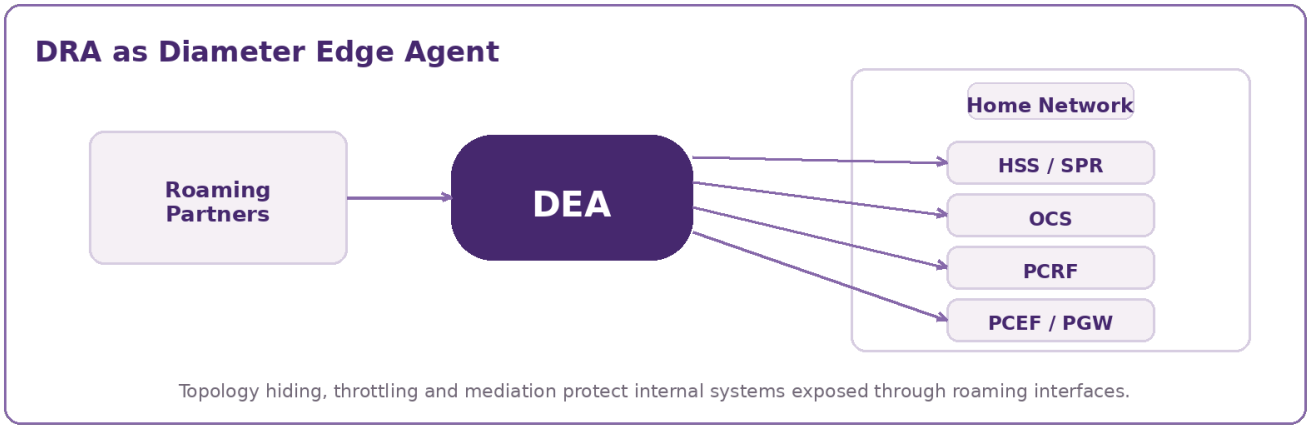
Network Topology Simplification

In a peer-to-peer signaling model, every new component can increase the number of Diameter relationships that must be configured and maintained. This creates operational risk during upgrades, migrations, capacity expansion and vendor replacement.

Introducing Cloud DRA centralizes these relationships. Network components connect to DRA, and DRA applies routing, mediation, session-binding and load-balancing logic according to operator policies.

Operational benefits

- Reduce the number of direct Diameter connections between network components.
- Add, replace or relocate network components with fewer topology changes.
- Apply routing rules consistently across Gx, Gy, Rx, Ro, Rf, S6a/S6d, Sy and other Diameter interfaces.
- Support traffic segmentation by subscriber group, service, region, MVNO or partner.
- Keep routing behavior consistent during phased migrations and network modernization.



Diameter Edge and Security Functions

When Diameter interfaces are exposed to external networks, roaming partners, MVNOs or partner domains, DRA can act as a Diameter Edge Agent. In this position, it controls the boundary between internal network systems and external signaling environments.

Cloud DRA can hide internal host and realm information, normalize signaling messages, throttle excessive traffic and apply routing rules before requests reach sensitive internal systems. This reduces operational and security exposure without changing the functional behavior of downstream network components.

Edge capabilities

- Topology hiding: remove or replace internal host and realm information in messages exchanged with external peers.
- External routing control: direct partner or roaming signaling to the right internal systems based on configurable policies.
- Overload protection: apply throttling and degraded-mode behavior during traffic bursts or component failures.
- Protocol normalization: mediate differences between vendor-specific Diameter dialects and attribute usage.

Cloud DRA: Core Functionality

Message Relay

Cloud DRA receives Diameter requests, selects the target component according to configured rules, forwards the message and returns the response to the originating component. If a target component becomes unavailable, DRA can redistribute requests to another available member of the same functional group.

Subscriber-Dependent Routing

Routing decisions can depend on subscriber identity, subscriber-profile information, home region, service group, MVNO, partner, or other attributes known to the operator. This makes it possible to segment traffic without duplicating subscriber data across every peer component.

Session Binding

For related interfaces and services, DRA can keep the same subscriber or session bound to the same target component. This is particularly important when different messages belong to the same policy, charging, voice or application session.

Degraded Mode

If downstream components fail or become overloaded, DRA can switch to a preconfigured degraded behavior. This may include temporary responses, traffic limitation, or rerouting to protect the wider network from cascading failures.

Mediation, Interworking and Load Control

Host / Realm Anonymizing

DRA can conceal internal host and realm names before messages leave the operator network. This protects the internal signaling topology from external peers and partner networks.

Mediation and Enrichment

Cloud DRA can modify, normalize or enrich Diameter AVPs according to operator rules. This supports compatibility between equipment from different vendors and allows messages to include subscriber or service context needed by downstream components.

Interworking

Where legacy or access systems still use RADIUS, Cloud DRA can support RADIUS-to-Diameter interworking. This allows operators to introduce Diameter-based signaling without replacing every dependent system at once.

Throttling

DRA can apply throughput limits for specific interfaces, peers, message types, destinations or subscriber groups. Throttling helps protect network components during peaks, failures, misconfiguration or unexpected traffic bursts.

Analytics, CDRs and Operational Visibility

A routing layer can provide valuable operational visibility because it processes messages crossing many Diameter domains. Cloud DRA can collect statistics, generate CDRs and provide KPIs for routing, performance, message distribution and component health.

CDR Generation

For selected Diameter interfaces, Cloud DRA can produce CDR records describing message history and session events. These records can be used for diagnostics, reporting, reconciliation, statistics and offline analysis.

KPI Collection and Metrics

Cloud DRA collects signaling statistics such as message volume, TPS, latency, success rates, response codes, peer availability and routing behavior. These metrics support operational dashboards, alerting and capacity planning.

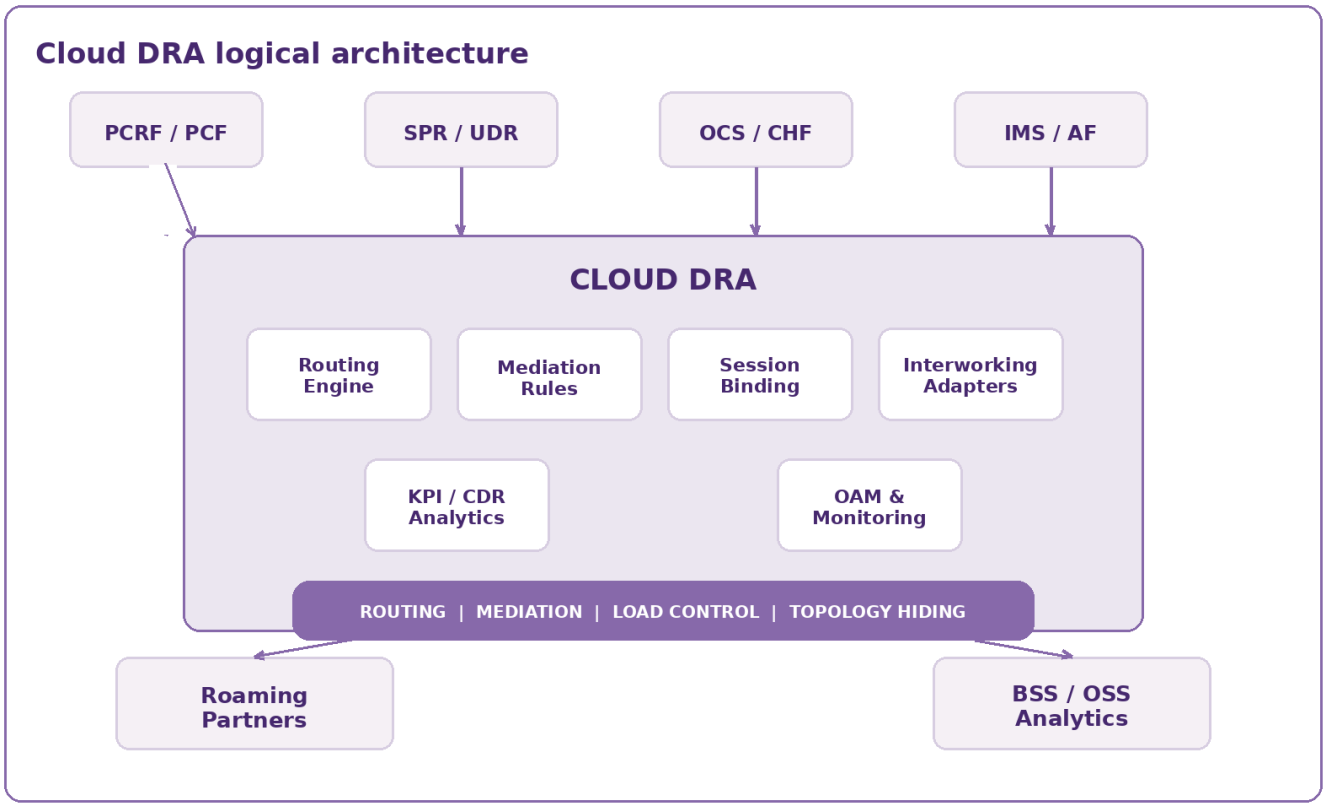
AI-Assisted Operational Analysis

Signaling data can also support advanced analytics. AI-assisted tools can help operators investigate unusual traffic patterns, identify routing anomalies, correlate signaling changes with network events and accelerate troubleshooting without replacing deterministic routing logic.

Cloud DRA: Architecture

Cloud DRA is built as a microservice-based, cloud-ready system. Its modules can run as autonomous services, interact over internal HTTP-based APIs and be scaled independently according to signaling load and operator requirements.

The architecture separates routing logic, message processing, mediation rules, session binding, adapters, OAM, monitoring and analytics. This separation allows operators to scale high-load components while maintaining operational visibility and resilience.



Deployment, Scaling and Resilience

Cloud DRA can be deployed on physical servers, virtual machines or cloud infrastructure. Operators can scale the deployment horizontally by adding processing nodes and distributing signaling traffic across available components.

High Availability

The solution supports redundant deployment patterns so that component failures do not interrupt signaling flows. If one processing node becomes unavailable, traffic can be redistributed to other available components according to routing and balancing rules.

Geo-Redundant Deployment

Cloud DRA can be deployed across multiple sites or regions to increase service availability and support disaster-recovery requirements. The design allows operators to protect critical signaling flows while maintaining flexibility in where routing and processing capacity is placed.

Monitoring and Operations

OAM, monitoring and service-discovery components provide visibility into module status, peer availability, routing behavior and system performance. Metrics can be exported to external monitoring and analytics systems.

Migration Support

During EPC, IMS, 5G NSA or multi-vendor migrations, Cloud DRA can be introduced as a stable routing point. This allows operators to change downstream systems progressively while keeping external or upstream integrations stable.

Standards, Interfaces and Specifications

Cloud DRA is designed around standardized Diameter signaling and integration practices used in telecom networks. The exact set of supported interfaces and applications depends on the operator architecture and deployment scenario.

Supported Diameter domains

- Policy and charging control interfaces such as Gx, Gy, Sy and Rx.
- Subscriber, authentication and mobility-related Diameter interfaces such as S6a/S6d where applicable.
- Charging, accounting and service-control interfaces such as Ro, Rf and related operator-specific variants.
- Roaming and edge scenarios based on Diameter Edge Agent deployment principles.

Reference specifications

- 3GPP Diameter Routing Agent: TS 29.213.
- 3GPP Subscription Locator Function: TS 29.228.
- IETF Diameter Base Protocol: RFC 6733.
- GSMA Diameter Edge Agent and S8/S6d proxy deployment guidance: IR.88.

Note: older Diameter base specifications have been superseded and should not be used as the main standards reference in current marketing materials.



globberry.com

info@globberry.com