4G/5G Packet Core KT

Supporting and maintaining LTE EPC and 5G core nodes in production

EPC and 5G Core networks consist of multiple interconnected nodes (e.g., MME, SGW, PGW, AMF, SMF, UPF) and it requires seamless interoperability in multi-vendor environment compliant with 3GPP standards.

Maintaining backward compatibility with older 2G/3G networks while integrating with 4G functionalities is complex. Frequent software updates, patches, and upgrades to address vulnerabilities or introduce new features can cause disruptions.

Diagnosing issues in real-time across multiple layers (radio, transport, core) and interfaces (like Uu, S1, S5, SGi, Rx, N2, N3) is time-sensitive and dynamically scaling network resources to handle traffic spikes, especially during events or emergencies, is critical.

Maintaining consistent configurations across distributed nodes to prevent mismatches and misconfigurations is a key challenge. Carrier-grade availability (99.999%) requires robust failover mechanisms, redundancy, and disaster recovery plans.

Adhering to national and international regulations, such as lawful interception and data privacy is a must. Managing and troubleshooting slices with different performance criteria could be complex.

3GPP call flows, example issues and mitigation

Symptoms: UE fails to attach; authentication request from MME/AMF times out.
DIAMETER_UNABLE_TO_COMPLY (5012): HSS cannot generate or deliver authentication vectors.
DIAMETER_ERROR_USER_UNKNOWN (5001): HSS does not recognize the IMSI or SUPI.
Mitigation: Verify IMSI provisioning in the HSS database. Ensure connectivity and routing integrity on the S6a/S6d (LTE) or N8 (5G) interface.

Symptoms: Incorrect QoS, service denials, or bearer establishment failures.
DIAMETER_AUTHORIZATION_REJECTED (5003): Subscriber profile rejects requested QoS or APN.
DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004): Subscriber restricted from accessing the requested network.
Mitigation: Audit and update subscriber profiles in the HSS. Align configurations between HSS and PCRF/PCF.

Symptoms: Frequent attach failures or dropped sessions.
DIAMETER_TOO_BUSY (3004): HSS is overloaded and cannot process requests.
DIAMETER_ERROR_INVALID_AVP_VALUE (5002): Invalid AVP (Attribute-Value Pair) in the Diameter request.
Mitigation: Balance traffic loads across redundant HSS nodes. Validate AVPs in Diameter messages for correctness and compliance with 3GPP specs.

Symptoms: Diameter message latency or failure.
DIAMETER_TOO_BUSY (3004): DSR or downstream nodes unable to handle signaling load.

DIAMETER_UNABLE_TO_DELIVER (3002): Message dropped due to unresolvable routing or congestion.
Mitigation: Scale DSR resources and optimize routing policies. Implement rate-limiting mechanisms to manage spikes in signaling traffic.

Symptoms: Repeated Diameter message retransmissions; no resolution of requests.
DIAMETER_LOOP_DETECTED (3003): Diameter message caught in a routing loop.
DIAMETER_INVALID_MESSAGE_LENGTH (5015): Misformatted messages due to routing issues.
Mitigation: Correct routing table and policy configurations in the DSR. Use signaling traces to identify and resolve routing loops.

Symptoms: Diameter transactions fail, or peers reject requests.
DIAMETER_AVP_UNSUPPORTED (5009): DSR cannot interpret or forward unsupported AVPs.
DIAMETER_MISSING_AVP (5005): Required AVP missing in the request.
Mitigation: Update DSR software to support the latest AVP standards. Add translation rules in DSR for custom AVP handling.

Symptoms: Registration failure; UE unable to establish PDU sessions - 4G/5G Hybrid context
403 Forbidden (HTTP/2 response code): UDM rejects data requests from AMF due to missing subscription.
DIAMETER_ERROR_USER_UNKNOWN (5001): SUPI not found in the UDM database.
Mitigation: Verify and sync SUPI-to-subscription mappings in UDM and UDR. Ensure correct N8 interface configurations and connectivity.

Symptoms: Incorrect QoS or slice allocation for UEs – 4G/5G Hybrid context
DIAMETER_AUTHORIZATION_REJECTED (5003): UDM denies session due to incompatible policies.
404 Not Found: Requested slice or profile not found in UDM.
Mitigation: Update and align policy configurations across UDM and PCF. Ensure NSSF slice data matches UDM configurations.

Symptoms: N8 communication fails; UDM cannot provide data to AMF.
TLS handshake failure: UDM and AMF certificates do not match.
504 Gateway Timeout: UDM cannot respond in time due to UDR or database latency.
Mitigation: Ensure proper certificate provisioning and validity. Optimize UDM-UDR query performance.

Symptoms: Delayed registration or session establishment due to slow UDR queries.
504 Gateway Timeout: UDR database fails to respond within the expected timeframe.
503 Service Unavailable: UDR under heavy load or unavailable.
Mitigation: Implement caching for frequently accessed data. Scale database resources or optimize query logic.

Symptoms: UE experiences intermittent service failures due to incorrect subscription data.
No specific Diameter or HTTP/2 error; manifests as indirect issues like registration failures.
Mitigation: Enable and monitor database replication to ensure consistency. Periodically audit UDR data for anomalies.

Symptoms: Security breaches or sensitive subscriber data exposure.
401 Unauthorized (HTTP/2 response): Invalid credentials for UDR access.
403 Forbidden: Access to specific data restricted due to policy violations.
Mitigation: Enforce strict RBAC and secure access controls. Regularly review and update UDR authentication and authorization policies.

Symptoms: UE fails to attach or register with the network; AUTHENTICATION FAILURE message observed in call flow.
LTE (S6a): *DIAMETER_ERROR_USER_UNKNOWN (5001)***:** IMSI/SUPI not found in HSS/UDM database. *DIAMETER_AUTHENTICATION_REJECTED (5003)***:** Incorrect authentication vectors or unauthorized access.
5G (Nudm): *401 Unauthorized (HTTP/2)***:** Invalid credentials or SUPI not provisioned.
Mitigation: Verify IMSI/SUPI in the HSS/UDM database. Check the cryptographic keys (K, K_asme) in the HSS/UDM and compare with UE credentials. Ensure the AMF/MME has the correct security algorithms configured.

Symptoms: Incorrect QoS, service denials, or bearer setup failures.
LTE (S6a): *DIAMETER_AUTHORIZATION_REJECTED (5003)***:** QoS or APN not allowed in the subscriber's profile. *DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)***:** Subscriber restricted from roaming.
5G (Nudm): *403 Forbidden (HTTP/2)***:** UDM denies access to requested QoS or slice.
Mitigation: Update subscription profiles in the HSS/UDM with the correct QoS and APN settings. Align network slice and policy configurations with the UDM and PCF.

Symptoms: Call drops during handover or TAU/RAU updates fail.
*LTE (S10/S11): CAUSE #15 (No Suitable Cells)***:** MME cannot find a cell to serve the UE.
*CAUSE #19 (Multiple PDN Connections for a Single APN)***:** Conflict in PDN session handling.
5G (N2/N3): *HTTP/2 404 Not Found***:** Requested network slice or data network not available.
Mitigation: Verify neighboring cell and tracking area configuration in the RAN and MME/AMF. Ensure PDN and slice configuration aligns across the core network and RAN.

Symptoms: Attach or bearer setup requests fail due to signaling timeouts or incorrect responses.
*DIAMETER_UNABLE_TO_DELIVER (3002)***:** DSR cannot route the message to the destination.
*DIAMETER_TOO_BUSY (3004)***:** Node is overloaded and rejects the request.
Mitigation: Validate routing configurations in the DSR (e.g., routing tables and realm settings). Scale DSR capacity or implement rate-limiting during high traffic.

Symptoms: UE unable to establish a session with the data network; no IP address allocated.
LTE (S6a/S5): *DIAMETER_ERROR_APN_NOT_ALLOWED (5007)***:** APN not permitted in the subscription profile. *CAUSE #27 (Missing or Unknown APN)***:** MME rejects the attach request.
5G (Nsmf): *403 Forbidden (HTTP/2)***:** SMF rejects session due to invalid slice or data network request.
Mitigation: Verify APN settings in the HSS/UDM. Ensure slice and data network configurations are provisioned correctly in the SMF and PCF

Symptoms: UE fails to attach while roaming; registration attempts rejected by the visited network.

LTE (S6a): *DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)***:** Roaming not permitted for the subscriber. *CAUSE #9 (UE Identity Cannot Be Derived)***:** IMSI/SUPI not recognized by the visited network.
5G (Nudm/Nssf): *403 Forbidden (HTTP/2)***:** Roaming denied due to invalid slice configuration.
Mitigation: Update roaming agreements and ensure correct configurations in the HSS/UDM and DSR. Check that the visited network supports the required slices or roaming capabilities.

Symptoms: Incorrect QoS or denied services during call or session setup.
LTE (Gx): *DIAMETER_AUTHORIZATION_REJECTED (5003)***:** PCRF denies requested QoS policy.
5G (Npcf): *403 Forbidden (HTTP/2)***:** PCF rejects QoS settings or slice request.
Mitigation: Synchronize QoS policies across HSS, PCRF/PCF, and RAN. Audit PCF configurations for correct policy enforcement.

Symptoms: UE fails to access the appropriate network slice.
*HTTP/2 404 Not Found***:** Requested slice unavailable in the UDM or NSSF.
*403 Forbidden (HTTP/2)***:** NSSF denies slice selection for the UE.
Mitigation: Verify slice configurations in the UDM and NSSF. Ensure correct SUPI-to-slice mapping and policy rules.

HSS and DSR Troubleshooting in Operation

Scenario: UEs are failing to attach to the LTE network, with repeated authentication rejections.
Diagnosis: Check the *S6a interface* between the *MME* and the *HSS*. Analyze Diameter messages using protocol analyzers like Wireshark. Look for errors such as:
*DIAMETER_ERROR_USER_UNKNOWN (5001)***:** *IMSI* not found in the *HSS*.
*DIAMETER_AUTHENTICATION_REJECTED (5003)***:** Incorrect authentication vectors provided.
Resolution: Ensure the IMSI is correctly provisioned in the HSS. Validate cryptographic keys and algorithms configured in the HSS match those in the UE. Monitor DSR routing to ensure proper delivery of S6a requests to the correct HSS instance.

Scenario: UEs are unable to establish a bearer due to APN configuration mismatches.
Diagnosis: Inspect the *Create Session Request/Response* messages from the MME to the HSS (S6a) via DSR. Typical error codes:
*DIAMETER_ERROR_APN_NOT_ALLOWED (5007)***:** The requested APN is not authorized for the subscriber. *DIAMETER_MISSING_AVP (5005)***:** Essential parameters like APN-OI are missing.
Resolution: Update the APN profiles in the HSS to include the missing APN. Configure the DSR with routing rules that ensure requests reach the appropriate HSS instance. Ensure DSR is appending necessary AVPs if required for downstream HSS compatibility.

Scenario: UEs cannot register while roaming in a visited network.
Diagnosis: Analyze Diameter signaling on the *S6a/S6d interface* between the visited network's MME and the home network's HSS via DSR. Common errors:
*DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)***:** Roaming restrictions in the subscriber profile. *DIAMETER_UNABLE_TO_DELIVER (3002)***:** DSR cannot route the Diameter message to the home HSS.
Resolution: Modify the roaming permissions in the HSS to enable roaming for the subscriber.
Update DSR routing tables to ensure messages are correctly routed to the home HSS.
Monitor and troubleshoot latency or congestion on the DSR affecting Diameter message delivery.

Scenario: Increased call setup delays and registration failures during peak hours.
Diagnosis: Check DSR logs for high CPU/memory usage. Look for:
*DIAMETER_TOO_BUSY (3004)***:** Indicates that the DSR is overloaded.
Dropped or delayed Diameter messages on critical interfaces (e.g., S6a, SWx).
Resolution: Scale up the DSR capacity by adding more nodes or increasing system resources. Implement traffic prioritization rules on the DSR to prioritize critical Diameter messages (e.g., authentication over billing queries). Optimize routing policies to distribute traffic evenly across HSS nodes.

Scenario: Incorrect *QoS* or bearer establishment due to policy mismatches.
Diagnosis: Check *Diameter* signaling on the *S6a interface* and analyze response codes from the *HSS*. Investigate *DSR* routing for potential misconfigurations leading to incorrect HSS responses. Look for errors like:
*DIAMETER_AUTHORIZATION_REJECTED (5003)***:** Subscriber policy mismatch.
*DIAMETER_UNKNOWN_SESSION_ID (5002)***:** Mismatched session state.
Resolution: Audit subscriber profiles in the HSS to ensure they align with network policies. Verify that the DSR is routing Diameter requests to the correct HSS instance based on policy requirements. Synchronize policy configurations across the PCRF, HSS, and DSR.

Scenario: Some UEs fail to attach or establish bearers in a network with multiple HSS nodes.
Diagnosis: Trace the Diameter messages through the DSR to ensure they are routed to the correct HSS. Identify misrouted requests and check for:
Incorrect *realm-based routing* in the DSR.
Missing or misconfigured *AVPs* **(***e.g., Destination-Realm, Origin-Host***).**
Resolution: Update DSR routing rules to correctly direct Diameter messages to the appropriate HSS node. Configure fallback mechanisms in the DSR to handle node failures. Monitor the Diameter traffic load on each HSS and balance it appropriately.

Scenario: UEs experience inconsistent behavior due to outdated subscriber data.
Diagnosis: Analyze synchronization between HSS and its replica instances (if any).
Inspect DSR logs for delayed or failed Diameter messages related to data synchronization.
Check for:
*DIAMETER_UNABLE_TO_COMPLY (5012)***:** Synchronization error in HSS.
Resolution: Verify that all HSS nodes are synchronized with the master database.
Configure DSR retry mechanisms to resend failed synchronization messages.
Audit DSR and HSS logs for system-level issues (e.g., connectivity, disk space).

Managing AAA and SMSC in Production

Scenario: Users are unable to connect to the network due to failed authentication.
Diagnosis: Check logs for authentication requests and responses.
Look for errors like:
*EAP Failure***:** Indicates an issue with Extensible Authentication Protocol (EAP) during RADIUS/DIAMETER transactions.
*DIAMETER_AUTHENTICATION_REJECTED (5003)***:** Invalid credentials or mismatched keys.
Analyze whether the issue originates from the UE, AAA server, or upstream systems (e.g., HSS).

Mitigation: Verify user credentials in the AAA database. Check communication between the AAA server and upstream authentication sources (e.g., HSS, UDM). Ensure correct configuration of supported authentication protocols (e.g., PAP, CHAP, EAP-AKA).

Scenario: Users are authenticated but cannot access certain services (e.g., data connectivity).
Diagnosis: Analyze RADIUS/DIAMETER logs for *authorization requests*.
Look for issues like:
*DIAMETER_AUTHORIZATION_REJECTED (5003)***:** Service or QoS policy not allowed for the user.
Missing AVPs (e.g., QoS Class Identifier, APN).
Check if user profiles in the AAA system align with service policies.
Mitigation: Update user profiles in the AAA database to include missing service permissions.
Sync policies between the AAA server and PCRF/PCF.

Scenario: Discrepancies in usage records between the AAA system and billing systems.
Diagnosis: Review accounting logs (e.g., RADIUS/DIAMETER Accounting-Request/Accounting-Response messages).
Check for missing or delayed accounting records.
Verify timestamps and session identifiers for consistency.
Mitigation: Ensure AAA server time synchronization with other network elements.
Optimize message retry and buffering settings in the AAA server to handle network delays.
Implement robust log rotation and storage policies.

Scenario: High traffic causes delayed responses or dropped authentication requests.
Diagnosis: Monitor AAA server resource utilization (CPU, memory, disk I/O).
Check for *DIAMETER_TOO_BUSY (3004)* or *RADIUS* retransmissions.
Mitigation: Scale AAA server resources or deploy additional instances. Implement traffic throttling or prioritization for critical requests. Use load balancing to distribute traffic evenly across AAA nodes.

Scenario: SMS messages are delayed during high traffic periods.
Diagnosis: Monitor SMSC queue lengths and processing times. Check for resource contention on the SMSC server (CPU, memory, disk I/O). Inspect signaling delays on MAP/Diameter interfaces to HLR or GMSC.
Mitigation: Optimize SMSC processing by upgrading hardware or scaling horizontally. Use rate-limiting to prevent overload during traffic spikes. Implement message prioritization for critical SMS (e.g., OTPs, alerts).

Scenario: Users receive multiple copies of the same SMS.
Diagnosis: Check SMSC logs for retransmissions caused by non-acknowledged deliveries.
Inspect the communication between SMSC and recipient network elements (e.g., MSC).
Mitigation: Configure SMSC retransmission settings to avoid unnecessary retries. Ensure proper acknowledgment handling in downstream nodes. Audit and correct timer configurations (e.g., message expiration).

Scenario: SMS messages fail when sent to or from other operators.
Diagnosis: Check SMSC logs for delivery attempts to external networks. Analyze routing configurations and look for errors such as:

Error 414 (Route Not Found): Incorrect or missing route to the destination operator.
Verify interconnection agreements and test routes.
Mitigation: Update SMSC routing tables to include missing routes. Coordinate with partner operators to resolve interconnection issues. Monitor route health and performance.

Scenario: Subscribers report inconsistencies in delivery status or duplicate messages.
Diagnosis: Check synchronization between SMSC nodes in multi-node setups.
Inspect replication logs for database updates.
Mitigation:
Resolve replication issues and ensure synchronization settings are correct. Schedule regular audits of SMSC database health.

KPI Analysis and Optimization

Definition: Percentage of successful UE attach requests to total requests.
Issue: Low ASR due to authentication failures.
Cause: Misconfigured credentials in the HSS/UDM or network congestion affecting the MME/AMF.
Mitigation: Verify UE credentials and synchronization with the HSS/UDM. Analyze S1AP and NAS signaling for errors like *DIAMETER_AUTHENTICATION_REJECTED (5003)*. Scale resources or optimize load balancing for the MME/AMF.

Definition: Percentage of successful PDN connections (bearer establishment).
Issue: APN not authorized for the user, reflected by *DIAMETER_ERROR_APN_NOT_ALLOWED (5007)* in HSS logs.
Mitigation: Update APN profiles in the HSS/UDM. Validate end-to-end routing for the requested APN.

Definition: Percentage of dropped sessions compared to total active sessions.
Issue: High CDR during mobility scenarios due to X2 or N2 handover failures.
Cause: Delayed or dropped signaling between MME/AMF and neighboring nodes.
Mitigation: Analyze handover signaling flows using tools like Wireshark. Optimize timer configurations for X2/N2 handovers. Address packet loss or latency in the backhaul network.

Definition: Percentage of sessions maintained successfully until termination.
Issue: Session drops caused by UE moving out of coverage or S1 interface issues.
Mitigation: Enhance coverage in weak signal areas. Resolve S1 interface congestion or hardware faults.

Definition: Time taken for a packet to traverse from UE to the application server and back.
Issue: High latency in 5G due to misconfigured QoS policies or congestion in UPF.
Mitigation: Verify QoS configurations in the PCF and ensure they align with SLA requirements. Analyze traffic distribution across UPF instances and rebalance as needed.

Definition: Average user data rate during a session.
Issue: Low throughput during peak hours caused by overloaded SGW/UPF.
Mitigation: Monitor SGW/UPF utilization and scale resources. Optimize bearer configurations for high-priority traffic.
Definition: Percentage of CPU/memory used by MME, AMF, SMF, UPF, or HSS/UDM.

Issue: High CPU usage in AMF causing signaling delays.
Mitigation: Scale AMF instances based on traffic patterns. Optimize signaling message retries and timers.

Definition: Bandwidth usage on critical links like S1, S6a, N2, and N3 interfaces.
Issue: Congestion on the N3 interface due to bursty traffic patterns.
Mitigation: Monitor traffic flows and implement QoS prioritization. Increase link capacity or deploy additional UPF instances.

Definition: Percentage of successful handovers (X2, S1, or N2).
Issue: Low HSR due to configuration mismatches between source and target cells.
Mitigation: Verify handover parameters in the source and target nodes. Test inter-node signaling to ensure compatibility.

Definition: Percentage of successful Tracking Area Updates.
Issue: Failed TAUs due to missing TAI in the HSS/UDM configuration.
Mitigation: Update TA mappings in the HSS/UDM. Resolve communication issues on the S6a/Nudm interface.

Definition: Percentage of successfully delivered SMS messages.
Issue: Low success rate due to routing issues in the SMSC.
Mitigation: Analyze SMSC logs for errors like *Error 211 (Absent Subscriber) or Error 412 (Invalid MSISDN)*. Update SMSC routing tables and verify interconnect agreements.

Definition: Percentage of allocated slice resources used.
Issue: Overutilization in one slice affecting other slices.
Mitigation: Monitor slice-specific traffic and resource allocation. Adjust slice quotas or deploy additional resources for overloaded slices.

Definition: Percentage of UEs meeting their QoS requirements.
Issue: QoS degradation for a specific application (e.g., VoNR).
Mitigation: Ensure accurate QoS mapping in PCF and UPF. Optimize scheduling algorithms in the RAN to prioritize critical traffic.