Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

BL0-100 Practice Questions
BL0-100 Practice Test
BL0-100 Practice Exam
BL0-100 Exam Questions
BL0-100 Study Guide

PASS

killexams.com

Nokia

BL0-100

Nokia Bell Labs 5G Foundation

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/BL0-100

Question: 447

An enterprise private 5G network automates end-to-end network slicing instantiation via intent-based API: customer portal submits createSlice(template="factoryURLLC", duration=12mo, sla={latency<5ms, rel=99.9999%}), triggering Digital Automation Cloud workflow provisioning RAN (gNB PRB quota 25%), transport (SRv6 path 1Gbps), core (UPF chain, PCF rules), validated against capacity (simulation 95th percentile), deployed (zero-touch config), assured (closed-loop SON monitoring). Manual equivalent requires 3 engineers 2 weeks. Which automation benefit quantifies this operational transformation?

A. Closed-loop automation reducing deployment time 100x with zero-touch
B. Static templates without real-time service assurance
C. Scripted automation requiring operator intervention per deployment
D. Manual configuration processes unchanged from traditional networks

Answer: A
Explanation: 5G automation implements intent-based networking (desired state API→observed state reconciliation): orchestration (Nokia DAC validates slice feasibility via digital twin simulation), zero-touch provisioning (ZTP NETCONF/YANG push to gNB/NF), closed-loop assurance (AI/ML analytics correlate E2E KPIs, auto-remediate PRB quota adjustment if P99>4ms), achieving 100x faster deployments (10min vs 2 weeks), 80% opex reduction, 99.999% SLA compliance. GitOps (ArgoCD, Flux) provides declarative config (one YAML change→fleet-wide rollout), AIOps (MantaRay) predicts failures 24h advance, transforming network ops from reactive firefighting to proactive service orchestration.

Question: 448

In a multi-story office building served by a 5G NR small cell with Nokia 128T128R advanced antenna system (AAS) operating at 3.8 GHz n77, the AAS applies independent vertical and horizontal beamforming to shape coverage: narrow horizontal beams (10° azimuth) for floor-level capacity and adjustable vertical tilt (5-15°) to illuminate specific stories without spillover. Capacity modeling shows 4x spatial layers per beam yielding 20 bps/Hz spectral efficiency (4 layers × 5 bps/Hz/stream via 64QAM). Which AAS capability directly enables this three-dimensional beam shaping and the resulting capacity gains in vertically distributed user scenarios?

A. Reliance on mechanical tilt for long-term coverage adjustments
B. Single-plane beamforming limited to azimuth sectoring only
C. Omnidirectional patterns for uniform building penetration
D. Three-dimensional beamforming with electronic tilt and azimuth control

Answer: D
Explanation: Advanced antenna systems (AAS) in 5G NR integrate massive MIMO arrays (128T128R dual-polarized elements) with full digital/hybrid control over both azimuth (horizontal) and elevation

(vertical) dimensions, enabling 3D beamforming where phase/amplitude per element forms narrow, dynamically shaped beams—e.g., 10° horizontal for capacity hotspots and 5-15° electronic vertical tilt to target floors 1-10 without illuminating unused space, reducing interference by 15 dB. This yields 4-8x capacity over 4G via SDMA (4 layers/beam), with Nokia AAS achieving 25-30 bps/Hz aggregate through real-time adaptation via CSI-RS feedback and precoding matrices (DFT/Type I codebooks). Unlike 4G passive antennas with fixed/mechanical tilt, AAS software-defined shaping (updated every 5-10 ms) optimizes for user distribution, boosting office throughput to 10 Gbps/sector.

Question: 449

Nokia's cloud-native 5GC platform uses containerized microservices (e.g., AMF pod with 8 vCPUs) orchestrated by Kubernetes, with Helm charts for CI/C**D.** During a load test simulating 1M UEs, PCF autoscales from 5 to 20 replicas based on CPU>70%, applying policy rules via N7 to SM**F.** 4G EPC VNFs scale monolithically via VMs. Which principle allows this granular, resilient scaling for peak-hour surges?

A. Cloud-native microservices with container orchestration
B. Vertical scaling through larger single-instance processes
C. Static hardware blades without virtualization support
D. Monolithic virtual network functions on dedicated hardware

Answer: A
Explanation: Cloud-native principles in 5GC implement NFs as microservices (lightweight, stateless, API-driven) in containers (Docker), orchestrated by Kubernetes (etcd for state, Istio service mesh for SBA traffic), enabling autoscaling (HPA/VPA), self-healing (pod restarts), rolling updates (zero-downtime), and CI/CD (GitOps). In the load test, PCF replicas query UDR (Unified Data Repository) for subscriber policies (e.g., Sponsored Data, Time of Day), distribute N7 load via NRF load-balancing—achieving 99.999% availability vs 4G EPC VM resize (minutes downtime). Nokia Reelhs uses CNFs with Helm3 for Day2 ops, supporting edge disaggregation.

Question: 450

In 5G cloud-native deployments, which security-related cloud-native principle helps protect network functions from lateral movement in case of compromise?

A. Shared credentials across all pods
B. No network segmentation inside the cluster
C. Zero-trust networking with mutual TLS (mTLS) enforced by service mesh (e.g., Istio) between microservices
D. Open network communication without encryption between functions

Answer: C

Explanation: Service mesh (Istio, Linkerd) injects sidecar proxies that enforce mTLS, authorization policies, and observability between microservices—implementing zero-trust even inside the Kubernetes cluster. This prevents lateral movement if one function is compromised. Open communication increases risk; shared credentials are insecure; segmentation is essential.

Question: 451

Smart metering network deploys 5 million NB-RedCap devices using preemptive mMTC: CG-Type1 (64 PRB periodic grant every 10min), small data integrity (6-bit MAC-I Msg3), and AI RACH optimization (backoff prediction 95% accuracy). Overhead reduces 85% versus LTE-M, capacity 5x. Which configured grant type eliminates scheduling request latency?

A. CG-Type1 autonomous periodic transmission
B. Contention-based CG with exponential backoff
C. Dynamic scheduling per transmission
D. CG-Type2 requiring DCI activation

Answer: A

Explanation: CG-Type1 (RRC configured PUSCH periodicity/time/freq resources) transmits autonomously without DCI activation or SR, ideal for periodic mMTC (soil sensors every 30min). Nokia validates 5M devices/km², 12-year battery life, versus Type2 4ms activation delay.

Question: 452

Kubernetes observability stack monitors 5G slicing: Prometheus scrapes NF metrics (AMF reg/sec, UPF Gbps), Grafana dashboards slice KPIs (P99 latency), Jaeger traces N11 latency distribution, Loki logs structured JSON. Alertmanager notifies on-call (P99>5ms → scale). Versus SNMP polling?

A. Console-only vendor dashboards
B. Log shipping without metrics
C. Full-stack observability with distributed tracing and alerting
D. Periodic SNMP counters without correlation

Answer: C

Explanation: Cloud-native observability (three pillars: metrics/logs/traces) enables 5G AIOps: Prometheus federation (10k series), OpenTelemetry auto-instrumentation (SBA spans), SLO/SLI calculation (error budget 0.1%). Nokia MantaRay correlates RAN+core+transport KPIs predicting slice degradation 1h advance.

Question: 453

End-to-end orchestration maintains strict binding between RAN sub-slice (gNB Slice Profile ID 14001), transport sub-slice (FlexE circuit ID 2001 with 1Gbps BW), and core network slice (S-NSSAI=010001) through explicit association maintained during lifecycle events (scale, heal). How does this mapping ensure service continuity?

A. Complete absence of sub-slice association mechanisms
B. Core-only mapping ignoring access network association
C. Strict end-to-end sub-slice binding across all domains
D. Loose coupling without domain association requirements

Answer: C
Explanation: E2E slicing employs sub-slice association (3GPP TS 28.541 Slice Profile→sub-slice identifiers) ensuring resource chains remain synchronized: RAN NSSMF configures gNB profile→maps to transport NSSMF circuit→core NSSMF NF selection. Orchestrator validates binding integrity during modification (e.g., scale RAN quota→proportionally adjust transport BW), preventing service degradation.

Question: 454

Which of the following statements correctly describe the primary benefits of deploying Segment Routing (both SR-MPLS and SRv6) in the 5G backhaul and midhaul transport network? (Select all that apply)

A. Source-based explicit path control that enables low-latency, slice-specific routing without maintaining per-flow state in intermediate nodes
B. Significant reduction in control plane signaling overhead compared to traditional RSVP-TE Label Switched Paths
C. Fast reroute mechanisms such as Topology-Independent Loop-Free Alternate (TI-LFA) achieving sub-50 ms protection switching for high-reliability services
D. Mandatory creation of a full-mesh of pre-provisioned LSPs between every pair of nodes, increasing operational complexity

Answer: A,B,C
Explanation: Segment Routing inserts a list of segment identifiers (SIDs) at the ingress node, allowing source-routed explicit paths for traffic engineering, low-latency steering (critical for URLLC slices), and network slicing isolation without intermediate node state—making it stateless and scalable. TI-LFA provides local repair with sub-50 ms convergence for link/node failures, supporting carrier-grade protection. SR eliminates RSVP-TE signaling for LSP setup/teardown, reducing control plane load and simplifying operations. Full-mesh LSPs are not required in SR; paths are computed dynamically or explicitly via controller, avoiding the complexity and scalability issues of traditional MPLS TE.

Question: 455

Which enhanced security feature in 5G protects against bidding-down attacks where an attacker forces the use of weaker cipher suites or older authentication methods?

A. Security capability negotiation during registration where the UE and network agree on the highest mutually supported security algorithms
B. Fixed use of null integrity and confidentiality algorithms
C. Elimination of algorithm negotiation entirely
D. No negotiation; fallback to weakest method is allowed

Answer: A
Explanation: During 5G registration, the UE sends its supported security capabilities (encryption/integrity algorithms). The network selects the strongest mutually supported set and signals it back. The UE verifies this selection matches its request, rejecting downgrades. This, combined with home network control in 5G-AKA, mitigates bidding-down—unlike 4G where downgrades were easier to force.

Question: 456

Which 5G security enhancement specifically addresses privacy concerns related to location tracking?

A. No location privacy features
B. Encrypted SUCI and frequent 5G-GUTI reallocation combined with obfuscation of location in exposed APIs
C. Cleartext location reporting
D. Permanent location exposure to third parties

Answer: B
Explanation: SUCI + GUTI changes prevent identity-based tracking. NEF exposure functions allow operators to anonymize or restrict location granularity for external applications.

Question: 457

A service provider virtualizes its 5G User Plane Function (UPF) using Nokia's NFV platform, replacing physical chassis with software instances running on COTS x86 servers equipped with SmartNICs (100 Gbps DPDK acceleration). Each VNF processes 200 Gbps forwarding (GTP-U decapsulation, QoS metering) with 10 µs buffering for URLLC slices. During peak traffic, vCPUs scale from 16 to 64 cores without service interruption. Which NFV capability fundamentally replaces dedicated hardware gateways while maintaining carrier-grade performance?

A. Container-only deployment eliminating virtual machine overhead

B. Physical appliances emulated through software abstraction layers
C. Network Functions Virtualization deploying VNFs on commodity hardware
D. Hardware acceleration cards within virtualized environments

Answer: C
Explanation: Network Functions Virtualization (NFV, ETSI NFV MANO) decouples network functions from proprietary hardware, implementing VNFs (Virtual Network Functions) as software on COTS infrastructure (x86 servers, SmartNICs) orchestrated by NFVO/VNFM/EM. UPF VNF leverages DPDK/VPP for kernel-bypass 200 Gbps forwarding (vector packet processing, 40 Mpps), SR-IOV VF assignment (32 queues per port), and NUMA-aware pinning (16 cores RU processing). Nokia Virtualized Service Router (VSR) achieves line-rate performance indistinguishable from physical, with heat-based autoscaling (vCPU + memory), live migration (no packet loss), and multi-tenancy (100 tenants/core), reducing capex 60% versus chassis-based UPFs while supporting 5G slicing isolation via VNF chaining.

Question: 458

A logistics operator compares 4G VoLTE bearers (QCI=1 GBR 30 kbps) and M2M APNs with 5G slicing for fleet tracking (mMTC Slice SST=3) and autonomous trucks (URLLC SST=1). 4G requires dedicated core (VoLTE MME/PGW), spectrum carve-outs; 5G shares infrastructure with S-NSSAI mapping. Which key difference highlights 5G slicing superiority over 4G approaches for multi-service efficiency?

A. 5G enables shared infrastructure slicing vs 4G dedicated elements/bearers
B. 4G slicing includes full RAN customization unlike 5G core-only
C. 4G supports unlimited slices like 5G with dynamic orchestration
D. Both use identical QCI/5QI without evolution

Answer: A
Explanation: 4G "slicing" approximates via QoS bearers (QCI 1-9) and APNs (logical PGW pools), but requires dedicated MME/SGW/PGW instances/spectrum for isolation (few slices, high cost); 5G true slicing (3GPP Rel15+) virtualizes e2e (shared RAN via slicing-aware DU, core NF instances, transport circuits) with virtually unlimited S-NSSAI (256+), dynamic instantiation (orchestrators). Logistics: 5G one infra serves mMTC (low prio, high density) + URLLC (preempt, survival) cost-effectively vs 4G dual nets.

Question: 459

Network slicing architecture implements hierarchical orchestration coordinating service orchestration (E2E OSS) with domain-specific controllers (RAN NSSMF, Transport NSSMF, Core NSSMF) configuring individual network elements via standardized southbound interfaces. Which management paradigm governs end-to-end slice lifecycle?

A. Domain-isolated management without coordination
B. Complete absence of orchestration requirements
C. Manual element-by-element configuration processes
D. Hierarchical end-to-end orchestration architecture

Answer: D
Explanation: Hierarchical orchestration (ETSI MANO, 3GPP TS 28.533) structures management: Service Orchestrator (intent capture, template selection)→Network Slice Subnet Managers (domain resource mgmt)→element managers (gNB OAM, transport NE config, 5GC NF instantiation). Nokia Digital Automation Cloud implements closed-loop lifecycle (design→deploy→assure→optimize→terminate), supporting 1,000+ slices with 99.999% reliability.

Question: 460

Which of the following represent key enhancements in 5G network access security compared to 4G LTE? (Select all that apply)

A. Retention of the same EPS-AKA protocol from 4G without any modifications
B. Introduction of the 5G Authentication and Key Agreement (5G-AKA) protocol providing mutual authentication, home network control, and protection against false base station attacks
C. Use of the SUPI (Subscription Permanent Identifier) with privacy protection via SUCI (Subscription Concealed Identifier) using public-key encryption
D. Mandatory integrity protection for user plane data in addition to confidentiality

Answer: B,C,D
Explanation: 5G-AKA improves over EPS-AKA by ensuring home network authentication of the serving network, stronger key derivation, and resistance to bidding-down attacks. User plane integrity is mandatory (optional in 4G), protecting against data modification in transit. SUCI encrypts SUPI using the home network public key (ECIES profile), preventing IMSI catchers from harvesting permanent identities —unlike 4G where IMSI was sent in cleartext during attach.

Question: 461

False base station detection: UE validates PLMN ID, signal strength anomalies, SUCI scheme negotiation failures. Active attack mitigation?

A. UE-side false base station detection mechanisms
B. Network-only detection
C. No rogue base station protection
D. Location verification only

Answer: A

Explanation: UE autonomous protection: PLMN mismatch abort, abnormal Tx power, ciphering downgrade detection. Nokia: 99.9% detection rate.

Question: 462

Nokia's cloud-native 5G Core deploys AMF as Kubernetes StatefulSet with 32 replicas across 3 AZs (Availability Zones), using etcd for distributed state (SUPI→AMF Set mapping) and Redis for session cache (P99 read 50 µs). During a DDoS attack flooding Registration Accept messages, Kubernetes Horizontal Pod Autoscaler spins up 50 additional pods within 45 seconds based on custom metrics (registrations/sec >100k/node), while NetworkPolicy drops malicious source IPs. Which container orchestration platform specifically enables this resilient, elastic scaling for stateful 5G control plane functions?

A. Bare-metal container runtime without orchestration
B. Virtual Machine Manager without container support
C. Docker Swarm limited to stateless container management
D. Kubernetes providing container orchestration and autoscaling

Answer: D

Explanation: Kubernetes orchestrates containerized 5G NFs through Deployments/StatefulSets (desired→actual state reconciliation), Horizontal Pod Autoscaler (HPA/Custom Metrics Adapter monitoring Prometheus 5xx/errors), Vertical Pod Autoscaler (VPA recommending resource requests), and Cluster Autoscaler (adding worker nodes). AMF StatefulSet maintains stable network identities (hostnames amf-0..31), PersistentVolumes (etcd snapshots), anti-affinity (spread 3 AZs), readiness probes (healthz/livenessz). Nokia CNFs leverage Helm charts (GitOps ArgoCD), service mesh (automatic mTLS for SBI N2/N11), achieving 10M registrations/sec cluster-wide versus VM-based VNFs requiring manual resize and 5+ minute downtime.

Question: 463

PCF branches: visited/home+AF input. Time/usage limits (e.g., 10 GB video). Dynamic vs Gx static. Intelligence?

A. Static GBR at setup
B. UE self-policy
C. No charging integration
D. Event-triggered policy updates

Answer: D

Explanation: N5 AF-SponsoredConnect, UDR events→PCC refresh 100 ms—usage-based throttle.

Question: 464

In a dense urban AR/VR hotspot requiring sustained 10 Gbps experienced throughput, which 5G advancements over 4G enable this eMBB performance? (Select all that apply)

A. URLLC grant-free access for low jitter
B. Massive MIMO and advanced beamforming for spectral efficiency gains
C. mmWave spectrum for abundant bandwidth in hotspots
D. Network slicing for traffic isolation but not peak rate increase

Answer: B,C
Explanation: Massive MIMO/beamforming boosts spectral efficiency, and mmWave provides wide bandwidths for multi-Gbps rates in hotspots, far beyond 4G sub-6 GHz limitations. Slicing ensures QoS but does not directly increase peaks; URLLC targets latency/reliability.

Question: 465

IPPM telemetry SRv6: IOAM (In-situ OAM) exports delay, loss, queue depth per hop. Postcard telemetry (BFD Echo) P99 latency monitoring. Assurance?

A. Passive SNMP polling only
B. In-situ path telemetry for microsecond visibility
C. End-to-end ping without hop detail
D. Manual traceroute testing

Answer: B
Explanation: SRv6 IOAM (RFC 9197) traces slice performance: proof-of-transit, edge-to-edge delay, 100K samples/sec. Nokia MantaRay correlates with RAN KPIs.

Question: 466

In Release 18 of the 5G specifications, which specific set of enhancements to ultra-reliable low-latency communication operation in unlicensed spectrum bands provides the highest level of reliability and deterministic performance while addressing the inherent contention and variable latency introduced by listen-before-talk procedures?

A. The complete restriction of ultra-reliable low-latency communication features to licensed spectrum bands only, with no support or extensions provided for unlicensed spectrum environments
B. The retention of the same unlicensed spectrum operation characteristics as defined in Release 16

without any further improvements for ultra-reliable low-latency communication use cases
C. The removal of all redundancy and repetition mechanisms when operating in unlicensed spectrum in order to minimize complexity and overhead
D. The extension of new radio unlicensed ultra-reliable low-latency communication with optimized listen-before-talk category selection, dynamic channel occupancy time adjustments, prioritized channel access mechanisms, and multi-transmitter multi-receiver redundancy configurations tailored for unlicensed operation

Answer: D
Explanation: Release 18 continues and significantly refines the Release 17 work on ultra-reliable low-latency communication in unlicensed spectrum (new radio unlicensed ultra-reliable low-latency communication). Key enhancements include the introduction of prioritized listen-before-talk categories that allow ultra-reliable low-latency communication traffic to gain earlier channel access compared to best-effort traffic, dynamic extension of channel occupancy time to reduce contention frequency, improved handling of listen-before-talk failures through adaptive backoff and fallback procedures, and the use of multi-transmitter multi-receiver redundancy schemes (such as packet duplication over different frequency resources or transmission points) to maintain the required reliability level of 99.9999% even in the presence of interference and contention. These features collectively enable deterministic performance in factory automation, logistics, and campus networks that prefer unlicensed spectrum for cost or spectrum availability reasons. Restricting ultra-reliable low-latency communication to licensed spectrum only would limit deployment flexibility, removing redundancy would degrade reliability, and retaining Release 16 behavior would leave significant gaps in unlicensed performance.

Question: 467

In Segment Routing deployments for 5G transport networks, which redundancy mechanism provides fast local repair in case of link or node failures while maintaining low-latency paths?

A. Long convergence times similar to traditional IP routing
B. Manual failover procedures requiring operator intervention
C. No redundancy mechanism available in Segment Routing
D. Topology-Independent Loop-Free Alternate (TI-LFA) protection achieving sub-50 millisecond convergence without requiring global signaling

Answer: D
Explanation: TI-LFA computes repair paths independent of topology, using SR SIDs to detour around failures locally with sub-50 ms protection—critical for URLLC and high-availability 5G services. SR inherently supports fast reroute; no manual intervention or long convergence is needed.

Question: 468

(Scenario) An enterprise deploys a private 5G network with dedicated slices for OT and IT traffic. Which 5GC components are deployed on-premises to ensure low-latency local breakout and data sovereignty?

A. AMF, SMF, UPF, UDM, PCF, and NSSF localized at the enterprise site
B. Complete elimination of UPF for private deployments
C. Only UPF localized, with control plane functions in the public cloud
D. Only RAN deployed locally, all 5GC in operator cloud

Answer: A
Explanation: For true private 5G with low latency, full control plane (AMF, SMF) and user plane (UPF) are deployed on-premises. UDM/UDR and PCF can be local or shared. NSSF ensures slice selection remains local. This avoids backhauling user plane to central cloud.

Question: 469

In a massive MIMO-based 5G NR deployment, which mechanism is primarily responsible for dynamically optimizing transmission reliability according to instantaneous radio conditions and UE capabilities?

A. Restriction to single-antenna transmission mode for simplicity
B. Complete elimination of CSI feedback to reduce signaling overhead
C. Rank adaptation combined with accurate channel state information (CSI) feedback that allows the base station to select the optimal transmission rank (number of spatial layers) and modulation scheme for each user
D. Fixed open-loop transmission without any adaptation

Answer: C
Explanation: Massive MIMO relies heavily on closed-loop operation using CSI feedback from the UE (via CSI reports including RI, CQI, PMI). Rank adaptation uses the reported rank indicator (RI) to dynamically adjust the number of spatial layers transmitted to a UE based on channel correlation, interference, and UE mobility. When channel conditions support high rank (low correlation), more layers are used for higher throughput; when conditions degrade (high correlation or interference), rank is reduced to maintain reliability. Accurate CSI enables this adaptation, ensuring robust performance across varying radio environments.