Carrier-Grade NAT (CGNAT) Port Block Allocation and Logging Best Practices - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

Carrier-Grade NAT (CGNAT), also known as Large Scale NAT (LSN) or NAT444, is a foundational technology for service providers facing IPv4 address exhaustion while transitioning to IPv6. This document defines best practices for port block allocation and deterministic logging on carrier-grade routing platforms. It provides engineering guidelines for maximizing subscriber density, ensuring lawful intercept compliance, and maintaining line-rate forwarding performance under sustained session loads.

The architecture described herein supports deterministic port block allocation (PBA), bulk port block logging, and high-availability failover without session loss. It is intended for pre-sales engineering, network architects, and compliance officers evaluating CGNAT deployment on carrier-grade hardware.



HARDWARE ARCHITECTURE & SILICON

CGNAT functionality is implemented directly in the forwarding ASIC and network processing units (NPUs) to avoid CPU-bound translation bottlenecks. The platform maintains separate hardware tables for inside subscriber mappings, outside global address pools, and port block descriptors.

Key silicon capabilities include:

- Hardware-accelerated NAT44 and NAT444 translation at line rate
- Dedicated TCAM/NPU memory for port block allocation state
- Deterministic port block sizing per subscriber (e.g., 1,024 ports per block)
- Concurrent IPv4/IPv6 forwarding with dual-stack CGNAT (DS-Lite, MAP-T)
- On-chip counters for session, port, and block utilization telemetry

Port Block Allocation (PBA) Best Practices

1. Block Size Selection: Allocate port blocks in powers of two (e.g., 512, 1024, 2048) to optimize hardware table utilization. Smaller blocks increase logging volume; larger blocks reduce subscriber density.

2. Block Reuse Policy: Implement round-robin or least-recently-used block recycling to prevent port exhaustion under churn. Retain idle blocks for a configurable quarantine period before reallocation.

3. Deterministic Allocation: Use a hash-based algorithm keyed on subscriber IP and internal port to ensure repeatable block assignment across failover events.

4. Port Range Reservation: Exclude well-known ports (0-1023) from dynamic allocation to avoid conflicts with critical services and simplify lawful intercept.

5. Dual-Stack Coordination: Align IPv4 port block allocation with IPv6 prefix delegation to maintain subscriber session consistency.

Logging Best Practices

1. Bulk Port Block Logging: Log block allocation and deallocation events rather

than per-session translations. A single log entry can cover thousands of flows, reducing logging volume by orders of magnitude.

2. Deterministic Timestamps: Use NTP-synchronized hardware timestamps with sub-second precision for all CGNAT log events.

3. Log Format Standardization: Emit logs in IPFIX, NetFlow v9, or syslog RFC 5424 format with mandatory fields: subscriber IP, global IP, port block start, port block end, allocation timestamp, deallocation timestamp.

4. Redundant Log Collection: Stream logs to at least two independent collectors over redundant management paths. Use TCP or TLS transport to guarantee delivery.

5. Retention Compliance: Retain CGNAT logs for a minimum of 12 months (or as mandated by local regulation) in tamper-evident storage.

[IMAGE_1]

KEY FEATURES & ROUTING LOGIC

- Deterministic Port Block Allocation: Hash-based block assignment ensures consistent subscriber-to-port mapping across line card failovers and chassis

restarts.

- Hardware-Accelerated NAT: Line-rate NAT44/NAT444 translation in silicon, with no forwarding performance degradation under full session load.

- Bulk Logging Engine: Generates block-level logs at wire speed, reducing log volume by up to 99% versus per-session logging.

- High Availability: 1:1 and 1:N redundancy models with stateful failover of port block allocations and active sessions.

- Lawful Intercept Support: Standards-compliant LI interfaces (ETSI, CALEA) with per-subscriber port block correlation.

- Dual-Stack Transition: Integrated DS-Lite, MAP-T, and NAT64 support for IPv6 migration strategies.

- Subscriber-Aware QoS: Per-subscriber policing and shaping applied post-NAT, preserving service level agreements.

- Comprehensive Telemetry: Streaming telemetry and SNMP MIBs for real-time port block utilization, pool exhaustion, and logging health.

COMPLIANCE & STANDARDS

The CGNAT implementation complies with the following standards and regulatory frameworks:

- RFC 6888: Common Requirements for Carrier-Grade NATs (CGNs)

- RFC 7422: Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT

- RFC 6302: Logging Recommendations for Internet-Facing Servers

- RFC 6264: An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition

- ETSI GS ISI 001: Lawful Intercept Handover Interface

- CALEA 47 CFR Part 1: Communications Assistance for Law Enforcement Act

- MEF 6.2: Carrier Ethernet Services

- ITU-T Y.1564: Ethernet Service Activation Test Methodology

TECHNICAL SPECIFICATIONS

Parameter	Specification
Form Factor	1RU / 2RU / 4RU Modular Chassis
Switching Capacity	Up to 12.8 Tbps (modular) / 3.2 Tbps (fixed)
Concurrent Subscribers	16,000 to 256,000 per platform
Port Blocks per Subscriber	Configurable: 512, 1024, 2048, 4096 ports
Block Allocation Method	Hash-based deterministic PBA per RFC 7422
Logging Method	Bulk port block logging (IPFIX / NetFlow v9 / syslog)

Log Throughput	Up to 100,000 block events per second
Power Supply	Dual Hot-Swappable Redundant AC/DC
Redundancy	1:1 and 1:N stateful failover, sub-second switchover
NAT Translation Performance	Line-rate, hardware-accelerated
IPv6 Transition Support	DS-Lite, MAP-T, NAT64, 464XLAT
Lawful Intercept	ETSI GS ISI 001 / CALEA compliant
Operating Temperature	0°C to 45°C (32°F to 113°F)
Management Interfaces	CLI, NETCONF/YANG, SNMPv3, Streaming Telemetry
Compliance	RFC 6888, RFC 7422, RFC 6302, MEF 6.2, ITU-T Y.1564

ORDERING SKU INFORMATION

Base Platform

- CGNAT-16K: 16,000 concurrent subscribers, 1RU, dual AC PSU

- CGNAT-64K: 64,000 concurrent subscribers, 2RU, dual AC/DC PSU

- CGNAT-256K: 256,000 concurrent subscribers, 4RU modular chassis, dual DC PSU

Logging & Compliance Options

- CGNAT-LOG-BULK: Bulk port block logging license (per 10K subscribers)

- CGNAT-LOG-LI: Lawful intercept logging and handover interface license

- CGNAT-HA-1:1: Stateful 1:1 high availability license

- CGNAT-DS: Dual-stack (DS-Lite/MAP-T) translation license

Transceiver & Interface Options

- SFP-10G-LR: 10G single-mode long-reach optic

- SFP-10G-SR: 10G multimode short-reach optic

- QSFP-40G-LR4: 40G single-mode long-reach optic

- QSFP-100G-LR4: 100G single-mode long-reach optic

