L02-network.json — Research Ledger

Purpose

This document is the persistent state artifact for the L02 network OSINT enrichment effort.
It exists because Claude's context window resets. Every finding, every dead end, every inference
and its rationale lives here so the next session can pick up without velocity loss.

Last updated: 2026-02-24, Session 1 (initial assessment)

---

1. SCHEMA (IMMUTABLE)

Entity fields: `id`, `entity_type` (always "network"), `name`, `description`, `zone`, `cidr`, `vlan_id`, `gateway`, `is_monitored` Relationship fields: `id` (UUID), `relationship_type`, `source_id`, `target_id`, `weight`, `confidence` Allowed relationship types in this file: `located_in`, `located_at`, `connects_to`, `supports`, `subject_to` Zones used: backbone, production, dmz, internal, corporate, external

CRITICAL: Schema cannot be altered. Confidence/source/rationale for entities goes IN the `description` field.

---

2. CONFIDENCE FRAMEWORK

Tier	Score Range	Label	Criteria
T1	0.85–0.95	OSINT-Verified	Direct observation from authoritative source (PeeringDB, ARIN, DNS, BGP)
T2	0.65–0.80	Strongly Inferred	Partial evidence + strong logical deduction (e.g., rDNS hints + product docs)
T3	0.40–0.60	Sector-Modeled	No direct evidence; inferred from company size, compliance requirements, industry norms
T4	0.20–0.35	Speculative	Plausible but minimal supporting evidence; included for completeness

Entity descriptions MUST include: `[CONFIDENCE: T1/T2/T3/T4]` tag and `Source:` or `Rationale:` citation.
Relationship confidence scores map to the same tiers numerically.

---

3. CURRENT ENTITY INVENTORY (55 entities as of Session 1)

3a. ASN/Backbone (11)

- net-001: AS12200 Global Backbone — VALIDATED
- net-002: AS33070 DFW — VALIDATED
- net-003: AS27357 IAD — VALIDATED
- net-004: AS19994 ORD — VALIDATED
- net-005: AS15395 LON — VALIDATED
- net-006: AS39921 UK Secondary — VALIDATED
- net-007: AS10532 SAT Origin — VALIDATED
- net-008: AS45187 HKG — VALIDATED
- net-009: AS58683 SYD/APAC — VALIDATED
- net-010: AS36248 US Supplementary — VALIDATED
- net-011: AS22720 AUS Dormant — VALIDATED

3b. IX Peering (17)

- net-018 through net-034: All from PeeringDB — VALIDATED
- Total IX capacity: ~455 Gbps aggregate

3c. DNS Infrastructure (4)

- net-035: Authoritative DNS (Anycast) — VALIDATED
- net-036: Cloud DNS (stabletransit.com) — VALIDATED
- net-037: Cloud Office DNS (name-services.com) — VALIDATED
- net-038: London Caching DNS — VALIDATED

3d. RackConnect Fabric (6)

- net-039: MPLS VPN Backbone — VALIDATED
- net-040 through net-044: Exchange fabrics — VALIDATED

3e. Email/SPF (5)

- net-017: AS396479 Mailgun — VALIDATED
- net-045: emailsrvr.com — VALIDATED
- net-048: Mailgun US — VALIDATED

- net-049: Mailgun EU — VALIDATED
- net-050: Corporate email (spf_a) — VALIDATED

3f. Corporate Infrastructure (4)

- net-051: DFW 72.3.128.0/24 — VALIDATED (127 rDNS hosts)
- net-052: IAD 69.20.0.0/24 — VALIDATED (55 rDNS hosts)
- net-053: LON 212.100.224.0/24 — VALIDATED (32 rDNS hosts)
- net-054: SAT/HQ 64.39.0.0/24 — VALIDATED (80 rDNS hosts)

3g. External/Other (8)

- net-012 through net-016: DataPipe acquired ASNs — VALIDATED
- net-046: stabletransit.com CP — VALIDATED
- net-047: AWS website hosting — VALIDATED
- net-055: ObjectRocket GCP — VALIDATED

---

4. IDENTIFIED GAPS (prioritized)

Phase 1: OSINT Enrichment (fact-findable)

Priority	Gap	Research Approach	Status
P1	CIDR enrichment for 25 empty entities	BGP looking glasses, ARIN/RIPE prefix lists	NOT STARTED
P2	Additional/missed ASNs	ARIN OrgId RACKS-8 search, RIPE ORG-RA33-RIPE	COMPLETE — found 4 new ASNs (AS398699, AS58982, AS200069, AS44009) + 5 sub-sets for future
P3	Cloud API endpoint networks	DNS resolution of *.api.rackspacecloud.com	NOT STARTED
P4	Additional rDNS corporate blocks	Sweep adjacent /24s to known corporate ranges	NOT STARTED
P5	Certificate transparency logs	crt.sh search for *.rackspace.com subdomains	NOT STARTED

Priority	Gap	Research Approach	Status
P6	Rackspace CDN/edge network	Akamai/CloudFlare integration points	NOT STARTED
P7	ORD/SYD/HKG corporate infra	rDNS sweeps for those DC regions	NOT STARTED
P8	PeeringDB update check	Verify no new IX peers since original capture	NOT STARTED
P9	Shodan/Censys banner data	Service fingerprinting on known IPs	NOT STARTED

Phase 2: Sector-Based Inference

Priority	Gap	Rationale	Status
S1	Out-of-band management networks	Every DC requires IPMI/iDRAC OOB; rDNS shows BMC at IAD	NOT STARTED
S2	DDoS mitigation segments	rDNS shows Arbor + Cisco Guard at DFW; dedicated segments standard	NOT STARTED
S3	Inter-DC dark fiber/DWDM	DFW-IAD-ORD triangle needs private transport at Rackspace scale	NOT STARTED
S4	Monitoring/NMS networks	rDNS shows rackwatch, MRTG, WhatsUp Gold; dedicated segments	NOT STARTED
S5	Cloud tenant overlay (SDN)	OpenStack Neutron / VMware NSX for multi-tenant isolation	NOT STARTED
S6	Customer VPN/remote access	Managed services delivery requires customer-facing VPN	NOT STARTED
S7	Backup/replication networks	DR requires dedicated replication paths between DCs	NOT STARTED
S8	FedRAMP boundary network	FedRAMP Moderate requires network boundary separation	NOT STARTED
S9	PCI DSS CDE segments	PCI Level 1 requires cardholder data environment isolation	NOT STARTED

Priority	Gap	Rationale	Status
S10	Staging/pre-production networks	Standard SDLC practice for service provider	NOT STARTED

5. RESEARCH LOG

Session 1 — 2026-02-24

- [x] Read and analyzed all 55 current entities
- [x] Categorized into 7 functional groups
- [x] Identified 25 entities missing CIDR data
- [x] Built gap taxonomy (9 OSINT + 10 inference priorities)
- [x] Established confidence framework (T1-T4)
- [x] Created this ledger
- [ ] BEGIN: Phase 1 OSINT research sprints

Session 1 Research Sprint: ASN Gap Analysis

AUTHORITATIVE SOURCE DISCOVERED: RADB AS-RACKSPACE as-set (bgp.he.net/irr/as-set/AS-RACKSPACE)

- Maintained by: MAINT-AS10532, admin Tom Sands, notify noc@rackspace.com
- Last changed: chris.hansell@rackspace.com 2023-11-09, RADB last-modified 2023-11-13
- This is the DEFINITIVE list of all Rackspace-controlled routing prefixes

AS-RACKSPACE RADB direct ASN members: AS10532, AS33070, AS27357, AS15395, AS36248, AS45187, AS19994, AS12200, AS58683, AS54535, AS39921, AS398699, AS58982

AS-RACKSPACE RADB sub-set members: AS-DATAPIPE, AS-LAYERED, AS-GOGRID, AS-FASTSERVERS, AS-ADAPT, AS200069

AS-RACKSPACE RIPE variant (ORG-RA33-RIPE) additional member: AS54636 (appears in RIPE but NOT RADB version — needs investigation)

NEWLY IDENTIFIED ASNs NOT IN OUR FILE:

1. AS398699 — In both RADB and RIPE AS-RACKSPACE. Owner TBD (likely Rackspace entity, needs ARIN lookup). **ADD**
2. AS58982 — DATAPIPE-SG-AP, DataPipe Singapore/APAC. APNIC registered, abuse@rackspace.com. Org: Rackspace Asia Ltd, Room 5101-5105, 51/F, Hopewell Center, 183 Queens Road East, HK. **ADD**

3. AS200069 — MAILJET SAS, Paris France. Rackspace subsidiary (Sinch Mailjet acquired post-Mailgun). ORG-MS158-RIPE. **ADD**
4. AS44009 — SLEEK-ASN, ORG-RA33-RIPE (Rackspace Ltd). AMS50 datacenter, transit from AS174/AS3549/AS6939. NOT in AS-RACKSPACE but registered to Rackspace RIPE org. **ADD**
5. AS54535 — CONFIRMED Nike Inc (NOT Rackspace). Customer transit recipient listed in AS-RACKSPACE for routing policy. **DO NOT ADD** as Rackspace entity.
6. AS54636 — Appears in RIPE AS-RACKSPACE but not RADB. Needs investigation. **DEFER**

Sub-set resolution needed (future sprint):

- AS-DATAPIPE: Should contain AS14492, AS16805, AS22205, AS22576, AS24778 (already in our file) plus possibly AS58982
- AS-LAYERED: Layered Technologies (acquired by RackSpace). ASN TBD.
- AS-GOGRID: GoGrid (acquired). ASN TBD.
- AS-FASTSERVERS: HostCentric/FastServers (acquired). ASN TBD.
- AS-ADAPT: Adapt/Datapipe (acquired). ASN TBD.

ALSO DISCOVERED:

- RIPE AS-RACKSPACE: ORG-RA33-RIPE, created 2017-02-09, last-modified 2022-11-04
- AS12200 bgp.he.net stats: 17 Internet Exchanges, 145 announced prefixes (139 v4, 6 v6), 191 BGP peers observed
- AS15395 (LON): 403,456 originated IPs — this is MASSIVE, much larger than documented
- AS19994 (ORD): 537,344 originated IPs, 85,429 hosted domains
- AS27357 (IAD): 259,840 originated IPs, 84,162 hosted domains
- AS45187 (HKG): 66,816 originated IPs, 36 BGP peers (much more connected than others)

DEAD ENDS (things we tried that yielded nothing — do NOT re-attempt)

- AS54535 looks like Rackspace but is actually Nike Inc (customer transit). Do not add.
- Direct BGPView API calls blocked by web_fetch permissions — use web search to scrape instead.

KEY DECISIONS

- Confidence embedded in description field (schema immutable)
- Entity IDs continue from net-056 onward
- Relationship UUIDs generated fresh per session
- All inferred entities get [CONFIDENCE: T3] or [CONFIDENCE: T4] prefix in description

- AS-RACKSPACE RADB as-set is the authoritative ASN inventory — cross-reference all future additions

---

6. NEXT SESSION PICKUP INSTRUCTIONS

When resuming this work:

1. Read THIS FILE FIRST — it has the full state
2. Read the current L02-network.json from /mnt/user-data/outputs/osint/ (or project)
3. Check Section 4 for the next gap to attack
4. Check Section 5 for dead ends to avoid
5. Continue entity IDs from the highest net-XXX in the file
6. Generate fresh UUIDs for relationships
7. Update this ledger with findings BEFORE outputting JSON