

PC-SAMPLE-NET-01 / EN / V1.1

Hybrid network design and cutover

ILLUSTRATIVE SAMPLE • FICTIONAL SCENARIO

PREPARED FOR
PREPARED

Orivane Industrial Group
2026-08-14

Network scope and service needs

This report presents an original fictional scenario. Orivane, its people, suppliers, systems, records and results are invented; established technology names identify the example stack only. No client material was used. Example hostnames use the reserved .example domain.

Orivane's Nacre network joins 18 business sites, Montréal datacenter MTL-DC1, Ashburn datacenter IAD-DC2 and three AWS regions. Jonah Patel owns NET-2608 and change CHG-2648. The network supports warehouse orders, office work, shared sign-in services and business applications. Connections must be predictable and recoverable. If a site fails, backup routes must preserve the same access restrictions.

The design separates user traffic, data replication, large transfers and administration. Capacity must cover measured peak demand when the primary connection fails. The advertised circuit speed alone does not prove this. Application dependencies must be mapped before scheduling the change.

DESIGN REQUIREMENT	ACCEPTANCE IMPLICATION
Controlled connections	Approved service flows work; forbidden cross-segment traffic remains denied during both normal operation and failover.
Predictable routes	Primary and alternate paths are explicit in both directions; no accidental equal-priority route controls a stateful flow.
Independent recovery	Out-of-band management and rollback authority remain available when the production path fails.
Observable failure	Monitoring separates transport loss, route loss, DNS failure and application failure.

Carrier procurement, physical cabling remediation and application redesign are excluded from the implementation scope. Any dependency on them becomes an explicit prerequisite with an owner, not an assumption buried in the change window.

Sites, carriers and the change record

MTL-DC1 occupies the Vela Quay campus in Montréal; IAD-DC2 occupies Stonebridge in Ashburn. They are additional to the 18 business sites below. Cloud hubs are ca-central-1, us-east-1 and eu-west-1. Jonah Patel operates; Amira Chen verifies; Tessa Lin accepts LedgerFlow transactions; Elias Moreno chairs the change window.

ESTATE	REGISTERED LOCATIONS
Canada	MTL-01 Montréal; QC-02 Québec; TOR-03 Toronto; OTT-04 Ottawa; HAM-05 Hamilton; YYC-06 Calgary.
United States	IAD-07 Ashburn; RIC-08 Richmond; CMH-09 Columbus; DTW-10 Detroit; PIT-11 Pittsburgh; BOS-12 Boston.
Europe	DUB-13 Dublin; ORK-14 Cork; LIM-15 Limerick; GWY-16 Galway; MAN-17 Manchester; RTM-18 Rotterdam.

Transport service register

PROVIDER	SERVICE AND OPERATING RECORD
Veyra Fiber	10 Gb/s private Ethernet per DC: VF-MTL-4401 and VF-IAD-4402. BGP local preference 200. Priya Nordin, service manager; incident VF-260814-06.
TernRoute Networks	5 Gb/s Internet per DC: TR-MTL-8821 and TR-IAD-8822, with IPsec to Nacre. Local preference 100. Mateo Silva, NOC lead; case TR-11842.
Mistral Mobile	Independent LTE management: MM-MTL-091 and MM-IAD-092. Elias Moreno holds recovery authority; login test OOB-0813.
Change window	CHG-2648: 22 August, 01:00-03:00 UTC. MTL-01 first; QC-02/TOR-03 after Tessa Lin's acceptance. Decision deadline 01:40 UTC.

Addressing, routing domains and dependencies

The prefixes below are an illustrative allocation plan, not an instruction to renumber an existing estate. Reconcile discovered ranges, partner routes, remote-access pools and container networks before reservation. A summary is advertised only when the advertising boundary owns its complete range and has a deliberate discard route for unused space.

DOMAIN	RESERVED BLOCK	SEGMENTATION RULE
Business sites	10.64.0.0/12	Subdivide by site and function; warehouse devices do not inherit office access.
Datacenters	10.80.0.0/12	Separate application, database and management route domains.
ca-central-1	10.96.0.0/12	Separate production, non-production and shared-service attachments.
us-east-1	10.112.0.0/12	Explicit inter-region application and recovery routes only.
eu-west-1	10.128.0.0/12	Same boundary contract; region presence grants no implicit reach.

Route policy

RP-17 controls route exchange through BGP. Orivane uses network identifier ASN 65010; the provider-facing identifiers are 64520/64530. Explicit lists limit accepted and advertised routes, with at most 200 prefixes per peer. Local preference ranks routes: 200 selects Veyra before TernRoute at 100. Set route preference by intended primary and backup paths, validate maximum-prefix limits, and document the handling of a default route. Do not allow a partner to inject a more-specific production route merely because it falls within an accepted aggregate. Route origin and business ownership must agree.

Before design freeze

Confirm address overlap, asymmetric return paths, network address translation ownership, maximum packet size and the source addresses seen by application allowlists. Each mismatch can invalidate a clean routing diagram. Record these as tested dependencies in the design register.

Network paths and access controls

This view follows approved cloud-bound service traffic. Veyra Fiber Ethernet and TernRoute IPsec reach the same Nacre regional policy contract. Neither path grants flat access across production, non-production or shared services. Return routing and inspection state must be verified for both paths.

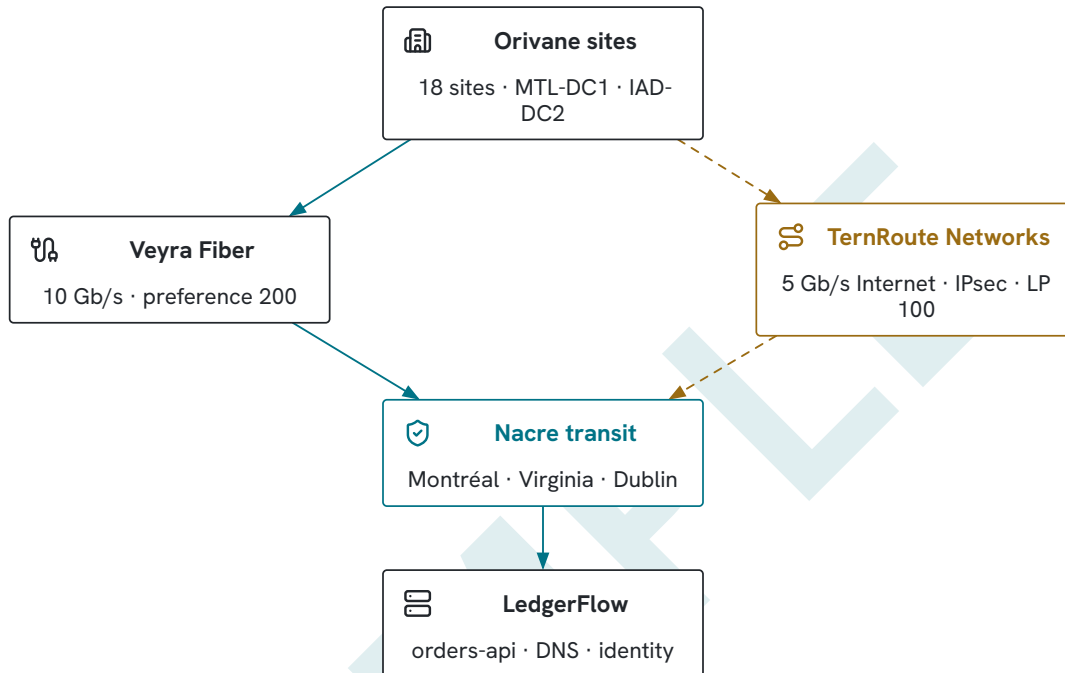


Figure 1 Veyra Fiber and TernRoute paths. Amber marks TernRoute's pending IAD duct-diversity evidence.

Required failure-path evidence

- ✓ The alternate carries peak failure load within agreed application limits.
- ✓ Allowed and denied flows retain the same policy in both directions.
- ✓ DNS, certificates and a business transaction work from actual source segments.
- ✓ Out-of-band access remains available when production transport is lost.

Service flows and DNS design

SOURCE	DESTINATION	PERMITTED PURPOSE
MTL-01 / VLAN 120	LedgerFlow API	10.64.1.0/24 → 10.96.10.0/24, TCP 443. No direct database or administrative session.
MTL-01 / VLAN 210	Orivane ID / nacre-dns-ca	Published authentication and resolver services; no general management subnet reach.
LedgerFlow API	ledgerflow-db	10.96.10.0/24 → 10.96.20.0/24, TCP 5432; symmetric inspection on return.
orv-recovery	LedgerSafe / ledgerflow-dr	Time-bound recovery flows with an owner and a defined closure step.
Non-production	Production	Denied unless a specific dependency is approved and represented in both route and firewall policy.

Name resolution is part of the path

Jonah Patel owns prod.orivane.example. MTL-DC1 forwards it to nacre-dns-ca at 10.96.0.10 and 10.96.0.11; us.orivane.example uses 10.112.0.10 and 10.112.0.11; eu.orivane.example uses 10.128.0.10 and 10.128.0.11. The DNS cache lifetime (TTL) drops to 60 seconds 24 hours before CHG-2648. A query for a cloud-private service must reach the regional resolver through an approved path and return the address intended for that consumer. Avoid reciprocal forwarding rules that turn an unknown zone into a loop. Record positive and negative caching behavior before moving records.

During migration, test from actual source segments with the production resolver chain. A successful lookup from an engineer's laptop does not validate warehouse clients or recovery hosts. Validate certificate names, application redirects and service discovery as well as address resolution. Keep old records only for the approved coexistence window.

Failure design and capacity proof

Two circuits are not independent merely because they have different invoice lines. Confirm entrance path, provider equipment, local power and upstream dependence. VF-DIV-0812 confirms separate Montréal entrances. TernRoute's IAD duct drawing DIV-118 is due from Mateo Silva on 18 August. Logical failover is accepted; physical independence at IAD is not.

FAILURE	EXPECTED RESPONSE	PROOF
VF-MTL-4401	Withdraw Veyra's path; prefer TR-MTL-8821 at local preference 100.	Route convergence, application success, session behavior and alternate-path utilization.
Inspection node	Use a healthy inspection path or stop affected traffic; never bypass policy silently.	Allowed and denied flow tests under failure, including stateful return traffic.
Regional resolver	Use the documented alternate without changing private-zone meaning.	Source-segment queries, cache expiry and application reconnect behavior.
Datacenter	Activate only approved recovery dependencies.	No broad route propagation; application owner validates the promoted service and data state.
Management path	Use the independent out-of-band channel.	Operator access, retained configuration and verified rollback authority.

Capacity test results

CAP-0812 sends 3.1 Gb/s through TR-MTL-8821. Packet loss is 0.08%; routes settle in 8.4 seconds; 95% of LedgerFlow responses arrive within 620 ms (p95). The limits are 0.1% loss, 15 seconds to settle routes, 900 ms at p95 and sustained tunnel traffic below 4 Gb/s. Include encryption and inspection overhead, large-packet behavior and competing replication traffic. Repeat CAP-0812 during CHG-2648; this rehearsal excludes simultaneous loss of both datacenters. A passing ping and an idle bandwidth test are insufficient evidence for a business cutover.

Go, hold or roll back

The change window has explicit decision points. A technical pass is necessary, and the application owner must accept service behavior before expansion. Any failed check stops the next cohort. Returning traffic also requires a compatible data state and an approved previous boundary.

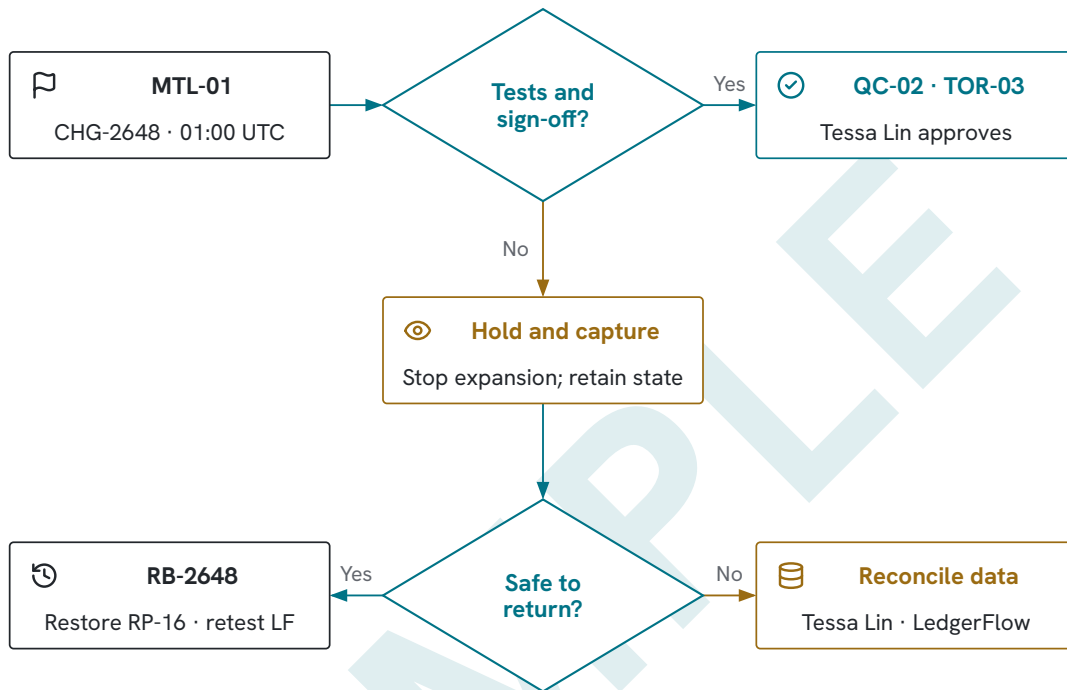


Figure 2 Decision deadlines leave time to restore service and check data consistency.

Before the operator starts

- ✓ Route intent, effective configuration and the rollback package are retained.
- ✓ Operator, verifier and application decision owner are present.
- ✓ The remaining window covers validation, a decision and a tested recovery path.

Cutover procedure

CHG-2648 begins at MTL-01 on 22 August, 01:00 UTC. Jonah Patel operates, Amira Chen verifies and Tessa Lin accepts the result. Elias Moreno records the 01:40 decision. The window closes at 03:00; RB-2648 begins by 02:10 to preserve 50 minutes for service validation.

POINT	ACTION	REQUIRED CHECKPOINT
21 Aug / 17:00	Freeze route intent, save effective configuration, check out-of-band access and complete a recovery rehearsal.	All prerequisite evidence accepted.
00:30 UTC	Confirm business readiness, current route state, monitoring baseline and absence of conflicting changes.	Change manager authorizes start.
01:00 UTC	Apply the prepared route and firewall change to the canary boundary only.	Second operator verifies effective state.
01:10 UTC	Run DNS, allowed and denied flow checks, then order LF-TEST-0822-0042 and its Dockline acknowledgment.	Application owner validates behavior.
01:25 UTC	Exercise the alternate path within the approved test scope.	No unexpected reach, loss or overload.
01:40 UTC	Admit QC-02/TOR-03, hold MTL-01, or invoke RB-2648.	Explicit decision recorded; no automatic expansion.

Do not compress validation to recover a late start. If the remaining window cannot accommodate verification and rollback, defer the next cohort. Preserve the observed state before troubleshooting changes so the second operator can distinguish the planned cutover from emergency edits.

Rollback and data-state limits

Rollback is triggered by unexpected cross-segment reach, loss of management access, sustained failure of an approved business test, or a failure-path capacity breach. The operator stops expansion, captures effective routes and policy counters, and informs the change manager. Restoring an old configuration is permitted only when its dependencies still exist and its risk remains acceptable.

A network rollback can redirect traffic, but it cannot undo writes, replicated state or messages accepted after cutover. If the application has changed its active data location, the application owner must authorize reconciliation before traffic moves back. This is a hold point even if the network team can revert in seconds.

STEP	VERIFICATION
Stop new cohorts	Freeze additional routing and DNS changes; keep one change authority.
Restore approved state	Reapply the reviewed previous policy and route preference, not a broad permit-all rule.
Reconcile sessions	Confirm stateful inspection, translated addresses and application reconnect behavior.
Validate service	Repeat allowed and denied flows plus a business transaction from the affected source segments.
Close the window	Record final state, unresolved symptoms, ownership and the next review before releasing staff.

The runbook includes a maximum decision time set during rehearsal. After that point, further troubleshooting requires explicit extension approval. The extension considers fatigue, remaining recovery time and business impact, not only whether the next command looks promising.

Handover evidence and operating checks

RECORD	CONTENTS
Design baseline	Address ownership, route import/export policy, approved flow matrix and dependency map.
Implementation	Reviewed configuration changes, effective before/after state and rollback package.
Acceptance	Source-specific DNS, allowed and denied traffic, business transaction and failure-path measurements.
Operations	Alert destinations, circuit identifiers, provider escalation, out-of-band access and maintenance ownership.
Exceptions	Overlap translations, retained legacy routes, untested failure domains and review dates.

Recurring checks

Alert on route count changes, unexpected default routes, tunnel health, resolver failure and loss of management reach. Schedule application-aware probes from representative sites. Rehearse failover after changes to routing, inspection, carrier service or application placement, and refresh the accepted baseline after review. A green circuit dashboard does not establish working business connectivity.

Assumptions still requiring evidence

The example assumes non-overlapping address ownership, available out-of-band access and application owners who can validate data state. CAP-0812 supports MTL failover. IAD physical diversity remains open in DIV-118; Jonah Patel must reconcile it by 18 August before the IAD wave. The [AWS Well-Architected Reliability Pillar](#) is a general recovery lens; it does not validate this fictional topology or supply its capacity targets.