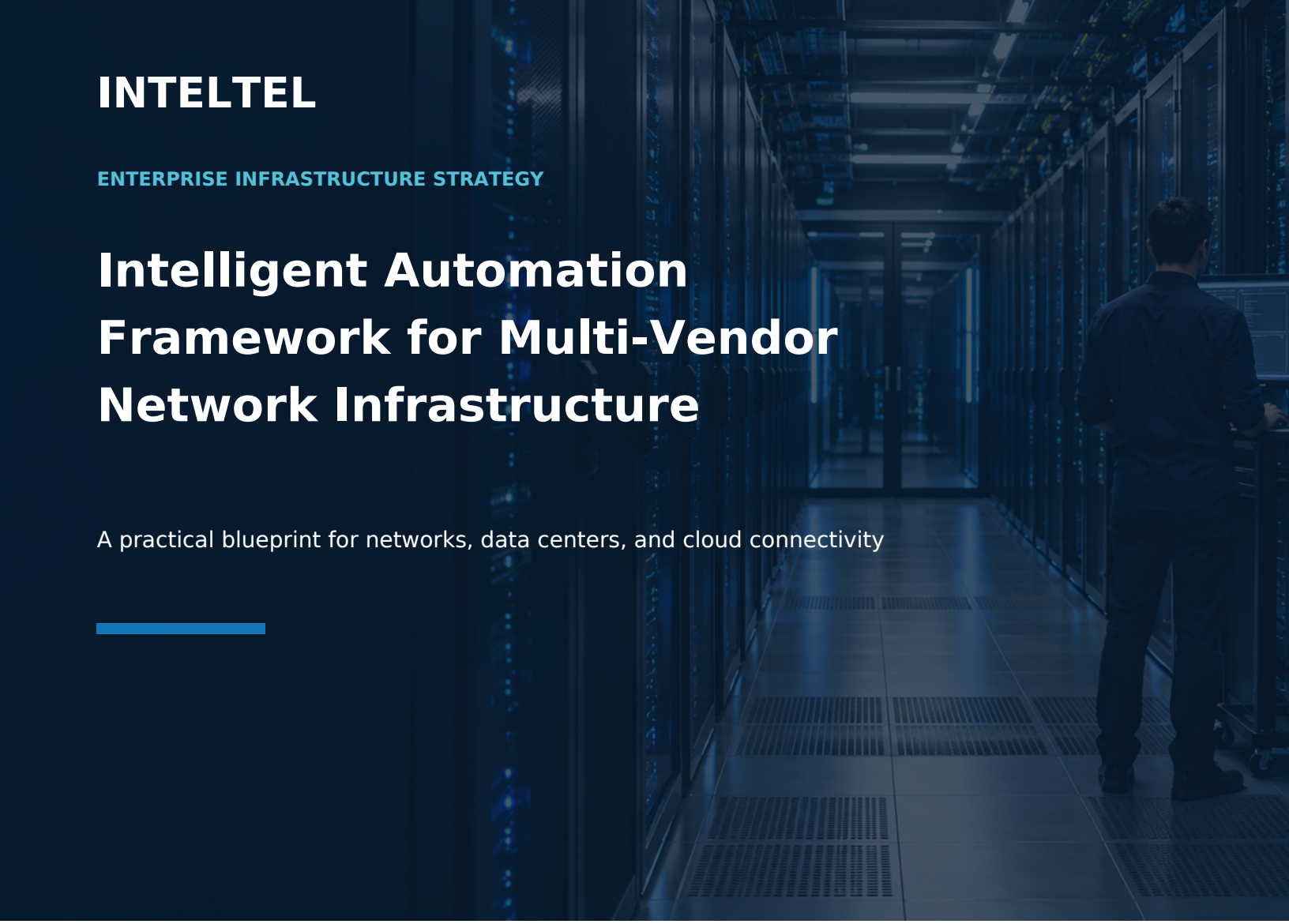
INTELTEL

ENTERPRISE INFRASTRUCTURE STRATEGY

Intelligent Automation Framework for Multi-Vendor Network Infrastructure

A practical blueprint for networks, data centers, and cloud connectivity



From fragmented tools to governed operations

Unify inventory, provisioning, telemetry, and policy across diverse platforms. Use AI to support fault detection and triage while keeping production changes controlled, auditable, and reversible.

ENTERPRISE OUTCOME

Consistent service delivery and visibility across branch, campus, data center, and cloud networks.

Why intelligent automation matters

Diverse vendors give enterprises flexibility but add configuration differences, separate consoles, and complex incident handoffs.

A unified operating model

Inteltel recommends a common layer for service intent, approved workflows, and operational evidence. Vendor-specific commands remain in tested adapters. Engineers retain ownership of change policy, exceptions, and service impact.

Faster delivery

Reusable request templates and staged execution remove repeated manual steps.

Higher change quality

Preflight tests, peer approval, verification, and rollback reduce avoidable errors.

Clearer accountability

Every workflow records its requester, scope, approver, outcome, and owner.

Stronger resilience

Correlated alerts and documented runbooks shorten investigation and recovery.

Where to begin

Start with reversible, high-volume tasks such as configuration backup, inventory reconciliation, and standard port provisioning. Expand only after pilot evidence supports the next risk level.

02 / ARCHITECTURE

A six-layer operating architecture

The framework separates authoritative data, service intent, execution, observability, analytics, and governance.

1 Source of truth	Device, site, circuit, service, ownership, and topology records.
2 Intent and policy	Approved templates, constraints, exception rules, and service standards.
3 Orchestration	Workflow control with vendor-aware APIs and device adapters.
4 Observability	Metrics, logs, configuration state, and service health.
5 Analytics	Event correlation, anomaly scoring, and recommended actions.
6 Governance	Identity, approvals, audit evidence, change control, and rollback.



Inventory and desired state

Reliable automation needs a versioned record of what exists, what each service requires, and what is approved to change.

Minimum source-of-truth fields

- Device identity: vendor, model, operating system, management address, role, site, and support state.
- Network context: interfaces, peers, circuits, VLANs, prefixes, routing domains, and dependencies.
- Service context: owner, application, criticality, maintenance window, and recovery objective.

Model the outcome, not only the command

Define a common schema for a VLAN, routing policy, access rule, or connectivity service. A tested adapter translates that model to each platform. Record vendor limitations as explicit exceptions so they cannot silently change service intent.

DATA QUALITY GATE

Reject an automated change when required attributes are missing, stale, or contradictory. Reconcile the inventory with discovery and configuration backups.

Enterprise control point

Designate an accountable owner for the inventory and define how acquisitions, new sites, cloud connections, and device replacements enter the model.

04 / EXECUTION

One controlled workflow across vendors

Standardize the lifecycle of a change even when syntax and APIs differ between devices.

Request	Select an approved service template and target scope.
Validate	Check inventory, access, support, dependencies, and policy.
Preflight	Capture current state, backup, reachability, and capacity.
Approve	Apply risk-based review and maintenance-window rules.
Execute	Run staged, idempotent tasks with bounded concurrency.
Verify	Compare operational state against declared intent.
Close	Retain diffs, logs, checks, and rollback evidence.

Priority workflows

Pilot standard VLAN and port changes, configuration backups, drift checks, and incident evidence packs. Stage software upgrades only after compatibility validation and a recovery rehearsal.

TOOLING EXAMPLE

The cited research combines Ansible, Nornir, and Netmiko. Platform selection should follow tested support, team capability, and security requirements.

05 / OBSERVABILITY

See the network as a service

Monitoring becomes actionable when device symptoms are linked to business services and their dependencies.



Metrics	Link, device, path, and service performance.
Logs and events	Fault context, policy threshold, and change correlation.
Topology	Upstream dependencies and potential blast radius.
Configuration	Drift and recent changes associated with incidents.
Traffic and capacity	Utilization trends and path shifts.

Operational view

Present health by site, service, and device role. Deduplicate related alarms before paging. Retain raw evidence and timestamps so engineers can inspect how a recommendation was reached.

Detect, explain, then act

AI can assist with anomaly detection and triage when recommendations remain inspectable and bounded by policy.

Advisory	Summarize evidence and recommend a runbook; engineer reviews.
Assisted	Prepare a scoped change with predicted impact; engineer approves.
Policy-governed	Execute only narrow reversible actions within preapproved limits.

Controls for production use

- Correlate independent signals before declaring a fault.
- Apply scope limits, rate limits, maintenance freezes, and a kill switch.
- Capture input evidence, model or rule version, action, and human override.
- Route low-confidence or high-impact decisions to an engineer.

SAFETY PRINCIPLE

A prototype result does not establish safe autonomous operation in a production enterprise network. Validate every action in a representative environment.

A safe recovery loop

Self-healing is a bounded sequence with verification and escalation, not an open-ended permission to reconfigure the network.

Detect	Confirm the symptom with telemetry and service checks.
Classify	Identify probable fault, affected services, and confidence.
Constrain	Check blast radius, change freeze, ownership, and policy.
Act	Use an approved reversible step or route to an engineer.
Verify	Confirm device state and end-to-end service restoration.
Escalate	Stop when recovery fails or uncertainty remains.

Recovery design

A known-good configuration restore, a prevalidated path change, or a collector restart may be appropriate in limited conditions. Every runbook needs a maximum attempt count, time limit, test, and exact rollback step.

FAIL-SAFE RULE

If post-change verification fails, revert automatically where supported and preserve evidence for the incident review.

Protect the automation plane

A platform with broad device reach must have strong identity, secrets, network access, and audit controls.

Least privilege

Separate read-only monitoring, discovery, change execution, and emergency identities.

Secrets

Store credentials in a managed vault; rotate them and keep them out of logs and code.

Change integrity

Require reviewed code, approved templates, and controlled releases.

Segmentation

Restrict controllers to permitted management interfaces and destinations.

Audit evidence

Retain request, approval, execution, validation, and rollback records.

Document vendor differences

Maintain a capability matrix for APIs, authentication, configuration transactions, rollback, telemetry, and rate limits. Label and approve fallbacks where behavior differs.

09 / DELIVERY

A phased implementation plan

Advance by demonstrated readiness and measurable outcomes rather than a calendar alone.

1 Baseline	Inventory, topology, metrics, and pilot device selection.
2 Standardize	Intent schema, templates, backups, and a test environment.
3 Pilot	Read-only visibility and low-risk change automation.
4 Expand	Additional vendors, sites, and staged service workflows.
5 Optimize	Assisted triage and narrow policy-governed recovery.

Pilot exit criteria

- Inventory and access are accurate for the selected scope.
- Jobs pass lab testing, peer review, and partial-failure scenarios.
- Verification and rollback are repeatable and documented.
- Operators can explain the alerts, actions, and service impact.

Test an unreachable device, failed API, stale inventory, and partially applied change before expanding to additional sites.

Prove business and operating value

Publish scorecard definitions and baselines before the pilot begins.

Change lead time	Approval to verified completion.
Automation success	Jobs with all post-change checks passing.
Rollback rate	Changes reverted after failed validation or impact.
Detection / recovery	Fault to detection and restored service.
Configuration drift	Assets outside approved desired state.
Adoption	Eligible work executed through standard workflows.

Research evidence and its limit

Rasul, Rahman, and Islam report more than 90% lower execution time and approximately 94-95% recovery success in a Cisco, Juniper, and MikroTik prototype. These are the authors' experimental findings, not Inteltel customer outcomes or enterprise production targets. Establish a separate baseline and measure your own pilot.

EXECUTIVE REVIEW

Report service impact, change quality, recovery performance, risk exceptions, and next investment decisions together.

Put the framework to work

An initial assessment identifies service priorities, estate diversity, operating constraints, and a credible first use case.

Inteltel engagement path

- Assess inventory quality, observability, change practices, support boundaries, and security controls.
- Select a low-risk automation pilot with measurable benefit and a tested rollback path.
- Design adapters, policy gates, dashboards, and ownership around the actual environment.
- Review pilot evidence with business and engineering leaders before expansion.

Research attribution

This Inteltel guide is an original advisory interpretation informed by Mirza Golam Rasul, Mst. Sahela Rahman, and Md. Rabiul Islam, "Intelligent Automation Framework for Multi-Vendor Network Infrastructure Using AI and Open-Source Tools," Middle East Journal of Applied Science & Technology, vol. 8, no. 4, pp. 118-128, published December 29, 2025. DOI: 10.46431/mejast.2025.8410.

The paper is cited for its architecture, tooling, and prototype findings. It does not describe an Inteltel deployment. Source: https://doi.org/10.46431/mejast.2025.8410

START A CONVERSATION

Inteltel.com | info@inteltel.com | 1-888-676-6261