Velsanet Identity White Paper

Network-Native Identity and Path Authority Model

1. Purpose

This document defines the identity model of the Velsanet architecture.

The purpose of this document is to specify how device identity is provisioned, interpreted, and enforced as a prerequisite for connection formation, independent of application semantics or data interpretation.

2. Scope

This document covers:

- identity provisioning at manufacturing time
- topology binding at deployment time
- presence detection and connection request generation
- identity-based path matching and formation
- post-formation validation and lifecycle handling

This document does **not** define:

- application protocols
- packet formats
- service orchestration
- data semantics

3. Design Principle

In Velsanet, connection authority is held by the network.

Devices do not select destinations, routes, or peers.
Devices submit identity attributes and connection constraints.

The network forms a connection only when the submitted attributes are structurally admissible.

Connection is not granted by permission.
Connection emerges from structural consistency.

4. Definition of Velsanet Identity

Velsanet Identity is a network-native structural identifier that defines:

- the maximum reachable topology domain of a device
- the hierarchy levels a device may access
- the conditions under which a device may occupy a path

Velsanet Identity is:

- not a locator
- not a session identifier
- not a user credential

Velsanet Identity is a constraint set evaluated by the network prior to and during path formation.

5. Identity Composition

A Velsanet Identity consists of the following elements:

- Region Code
- Hierarchy Level Code
- Device Role Code
- Path Constraint Profile

Together, these elements define the admissible connection domain of the device.

6. Identity Provisioning (Manufacturing Stage)

Velsanet Identity is provisioned during manufacturing.

At this stage, the device is embedded with:

- predefined region and hierarchy identifiers
- a hardware root of trust
- cryptographic keys for attestation

Identity provisioning is mandatory and precedes any network attachment.

No dynamic identity creation occurs at first connection.

7. Topology Binding (Deployment Stage)

Upon deployment, the region code embedded in the device is bound to an actual Velsanet topology region.

This binding transforms identity from a symbolic descriptor into a topology-constrained identity.

After binding, the device is limited to the admissible network scope defined by its identity.

8. Presence Detection

Network presence is detected through physical signal activation.

- wired devices: optical termination activation
- wireless devices: radio channel occupation

Presence detection establishes the existence of a connectable entity.

No destination, service, or session is defined at this stage.

9. Connection Request Generation

After presence detection, the device generates a connection request.

The request includes:

- Velsanet Identity
- device role
- required path constraints

Path constraints may include, but are not limited to:

- latency bounds
- continuity requirements

- isolation level
- synchronization requirements

No application-level semantics are included.

10. Edge Validation

Access-level nodes perform initial validation of the request.

Validation includes:

- identity syntax verification
- region and hierarchy consistency checks
- admissibility of requested path constraints

Requests failing validation are rejected prior to entering higher network layers.

11. Path Matching and Formation

The network evaluates validated requests against available cores, planes, and paths.

If a structurally admissible match exists, a path is formed.

Path formation operates at the core and plane level.
No packet-level routing decisions are involved.

12. Post-Formation Attestation

After path formation, attestation is performed to verify:

- authenticity of the device identity
- correctness of topology binding
- compliance with hierarchy and constraint rules

If attestation fails, the path is downgraded or terminated.

13. Path Maintenance

Formed paths are maintained as stateful entities.

Reconfiguration may occur due to:

- topology changes
- constraint updates
- fault conditions

Reconfiguration is constrained by the original identity and path constraints.

Devices do not directly control reconfiguration.

14. Path Termination and Record

When a connection terminates, the path is released.

A record of:

- identity
- constraints
- path usage

is retained for auditing and verification purposes.

15. Summary

In Velsanet:

- identity defines admissible connectivity
- connectivity is formed through structural matching
- trust is replaced by topology-constrained path authority

Identity, authority, and path formation are inseparable.