Intentional Disconnect Mode

by Nick Clark | Published April 25, 2026

What It Specifies

Intentional-disconnect mode is governance-credentialed. The disconnecting authority, the disconnect duration, the disconnect reason, and the disconnect parameters all enter lineage; the mesh operates within the declared disconnect mode.

Reconnection is also credentialed. The reconnecting authority, the reconnection-reconciliation, and the resulting state all enter lineage; downstream operations admit the reconnection structurally.

Why It Matters Structurally

Cross-mesh integration without intentional-disconnect support produces architectural rigidity. Real operations require deliberate disconnection (defense covert, regulatory isolation, security containment); the architecture must support the disconnection.

Intentional-disconnect mode produces structural support. Disconnection becomes a declared operating state; reconnection follows declared protocols; outcomes are auditable.

How It Composes With Mesh Operation

The architecture defines the disconnect-mode protocol, the disconnect-state operation primitives, and the reconnection-reconciliation handling. Implementations apply the architecture; disconnect operations proceed within the framework.

Disconnect composes with other features. Cross-jurisdictional intentional disconnect, byzantine-robust disconnect under disputed authorization, and dispute mechanism for disconnect disputes all build on the disconnect primitive.

What This Enables

Defense covert-operations cross-mesh operations gain structurally-supported intentional disconnect. Civilian regulatory-isolation operations gain the same.

The architecture also supports disconnect evolution. As disconnect patterns are characterized through operational experience, disconnect protocols update through governance procedures.