Nebula Built Overlay Mesh Networks. The Certificate Authority Is Still Central.

by Nick Clark | Published March 28, 2026 | PDF

Nebula, created at Slack and open-sourced, builds encrypted overlay mesh networks where each node receives a certificate from a central certificate authority defining its identity, group membership, and allowed IP range. Nodes communicate directly through peer-to-peer tunnels without routing through a central server. The mesh operates without a central data path. But the certificate authority that defines identity and group membership is central. If the CA is compromised, every node's identity is compromised. The gap is between peer-to-peer mesh transport and protocol semantics where identity and trust authority are intrinsic to each node's accumulated behavior.

Nebula's combination of certificate-based identity with peer-to-peer encrypted communication is elegant engineering. The lightweight binary and cross-platform support make deployment straightforward. The gap described here is about the identity and trust authority model, not about mesh connectivity.

Identity defined by certificate, not by behavior

Each Nebula node's identity is defined by a certificate signed by the CA. The certificate specifies the node's name, IP address, group membership, and validity period. The node proves its identity by presenting its certificate. Identity is what the CA says it is.

If a certificate is compromised, the node's identity is compromised. If the CA key is compromised, all identities are compromised. The certificate model concentrates identity authority in a single signing key. The mesh is decentralized for transport but centralized for identity.

Firewall rules enforce group-based policy statically

Nebula's firewall rules control which groups can communicate with which groups on which ports. These rules are defined in each node's configuration file. The rules are static: they do not adapt to network conditions, trust changes, or governance requirements. A node in the "servers" group can communicate with nodes in the "monitoring" group because the configuration says so, not because the protocol dynamically evaluates trust.

What memory-native protocol semantics provide

A memory-native protocol would embed trust authority in the protocol itself. Each node's identity would derive from accumulated behavioral continuity, not from a static certificate. Routing policy would travel with each packet, evaluated dynamically based on the content's trust scope and the receiving node's governance requirements.

Nebula's efficient peer-to-peer tunneling could serve as the transport layer. The memory-native protocol above would provide dynamic identity, semantic routing, and governance that adapts to network conditions rather than static certificate and firewall configurations.

The remaining gap

Nebula built lightweight overlay mesh networking with certificate-based identity. The remaining gap is in the protocol layer: whether identity and trust can be protocol-intrinsic properties derived from behavior rather than static certificates issued by a central authority.

Memory-Native Protocol All 21 steps →

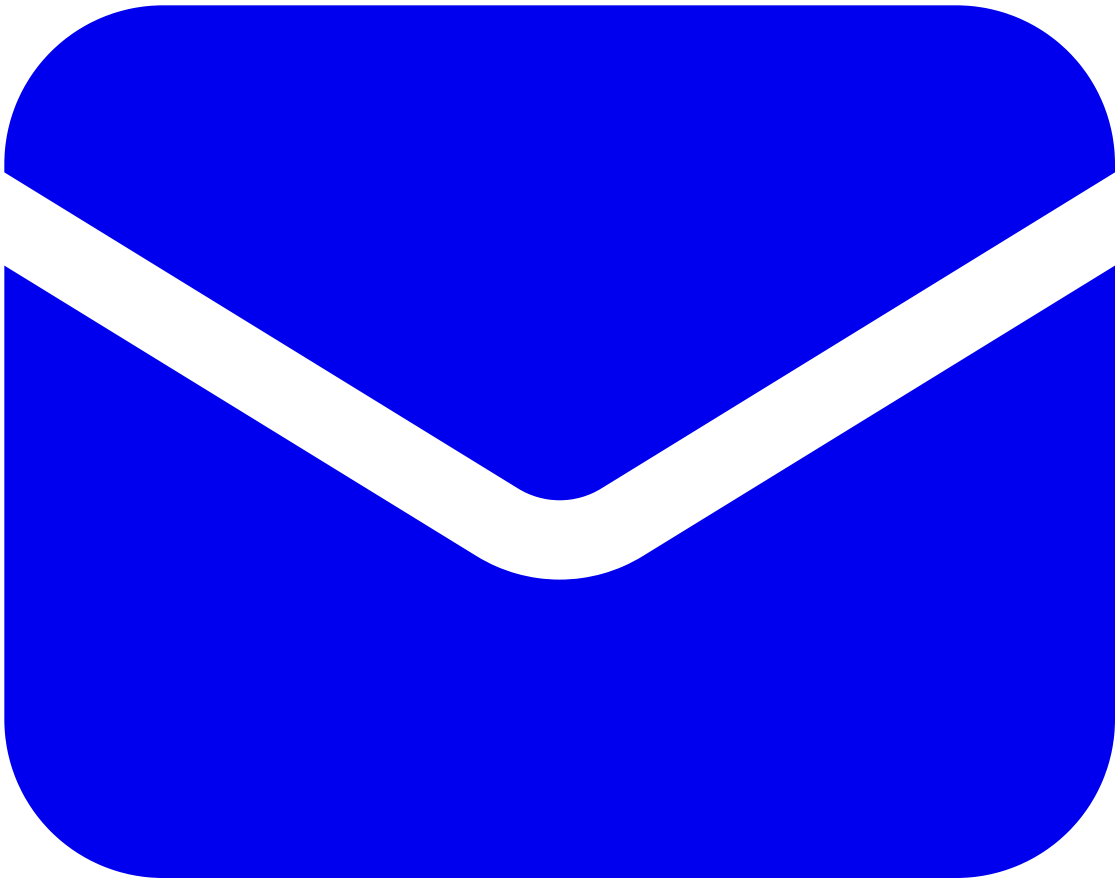
Authority intrinsic to the object. Routing by semantic properties.

Patent
US 19/366,760 · filed
Primary Technical Disclosure
○ Memory-Native Networking: A Cognition-Compatible Protocol Substrate
Secondary Technical
○ Protocol-Native Carriers: Agents as the Fundamental Unit of Transmission○ Dynamic Routing Protocol: Memory-Aware Path Selection for Semantic Agents○ Trust-Weighted Route Scoring: Dynamic Path Selection Through Policy-Defined Trust Thresholds○ Network Health Monitoring System: Signed Health Agents as Distributed Operational Telemetry○ Health Agents as Semantic Objects: Operational Metrics That Route Like Any Other Agent○ Dynamic Indexing Protocol: Entropy-Driven Restructuring of Semantic Flows○ Soft-Index Anchors: Ephemeral Index Points Inferred From Agent Lineage○ Adaptive Consensus Protocol: Memory-Native Quorum Without Fixed Validator Sets○ Trust-Weighted Voting in ACP: Domain-Scoped Votes Accumulated Against Agent Memory○ Dynamic Alias Resolution: Zone-Local Semantic Aliases Resolved Through Transport Headers○ Horizontally Composable Protocol Stack: Independent Layers Operating in Parallel○ Transport-Layer Agnosticism: One Protocol Stack Above Any Carrier○ Federated Semantic Zone Deployment: Heterogeneous Nodes Coordinating Across Trust Boundaries○ Health-Triggered Quorum Adjustment: Dynamic Thresholds From Network Stability Signals
Applications (General)
○ Edge Computing Without Central Routing Authority○ IoT Device Mesh Governance at Scale○ Vehicle-to-Vehicle Communication With Intrinsic Governance○ Military Mesh Networks Without Central Routing Authority○ Smart City Infrastructure With Self-Governing Transport○ Satellite Communication With Delay-Tolerant Governance○ Industrial IoT Protocols With Embedded Authority○ Healthcare Device Mesh Networking
Applications (Specific)
○ Starlink Built a Satellite Mesh. The Routing Authority Is Still Terrestrial.○ Zigbee Built a Mesh Protocol for IoT. The Messages It Carries Have No Memory.○ Matter Unified Smart Home Devices. The Protocol Still Separates Data From Authority.○ Helium Decentralized Wireless Coverage. The Protocol That Uses It Did Not Follow.○ LoRaWAN Solved Long-Range IoT. The Messages Are Still Passive Payloads.○ Tailscale Made WireGuard Usable. The Coordination Server Still Holds the Authority.○ QUIC Modernized Transport. The Protocol Carries No Semantic Authority.○ MQTT Connected Billions of IoT Devices. The Broker Still Holds the Authority.○ CoAP Brought REST to Constrained Devices. The Protocol Carries No Governance Semantics.○ gRPC Made Service Communication Type-Safe. The Protocol Carries No Trust Semantics.○ ZeroMQ Eliminated the Broker. Routing Authority Still Lives in Application Code.○ WireGuard Simplified VPN Tunnels. The Protocol Has No Semantic Routing Layer.● Nebula Built Overlay Mesh Networks. The Certificate Authority Is Still Central.○ Calico Enforces Network Policy at the Kernel Level. Policy Authority Is Still External.○ Cilium Made eBPF the Network Data Plane. The Protocol Layer Carries No Governance.○ Weave Net Built a Virtual Network for Containers. The Protocol Carries No Semantic Authority.
Memory-Native Protocol overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03

-
- Inventive Steps
- Licensing
- Patents
- Articles
- Legal
- Opportunities
- Sitemap



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie