Dynamic Routing Protocol: Memory-Aware Path Selection for Semantic Agents

by Nick Clark | Published March 27, 2026 | PDF

Memory-aware routing layer scoring candidate paths using trust information from agent memory fields, network health signals, and semantic scope constraints rather than address-based forwarding. Within the memory-native protocol stack, this capability operates as a structural primitive at the transport level. It is not an optional enhancement or a configurable plugin but a mandatory architectural property that every participant encounters. The result is a system where dynamic routing protocol (drp) is enforced by construction rather than by convention, policy, or external oversight.

What It Is

Memory-aware routing layer scoring candidate paths using trust information from agent memory fields, network health signals, and semantic scope constraints rather than address-based forwarding. This is a structural mechanism within the memory-native protocol stack that operates at the transport level. It is not advisory, not configurable at the discretion of individual participants, and not dependent on external enforcement infrastructure.

Every interaction within the system encounters this mechanism as a mandatory constraint. The behavior it produces is deterministic: given the same inputs and the same system state, the outcome is identical regardless of which node evaluates it, when the evaluation occurs, or what substrate hosts the computation.

Why It Matters

Conventional networking protocols address this problem through external policy layers, firewalls, and middleware. These approaches function adequately under controlled conditions but introduce structural fragility when systems scale beyond a single administrative domain or operate under partition. The underlying assumption that a central authority can inspect and govern all traffic becomes a liability precisely when reliability matters most.

Dynamic Routing Protocol (DRP) removes this fragility by embedding the relevant capability directly into the transport layer. There is no external dependency that can fail independently, no middleware that can be misconfigured, and no trust assumption that can be violated by a single compromised participant. The guarantee is structural.

How It Works

The mechanism operates through deterministic evaluation embedded in the memory-native protocol stack. When a relevant operation is initiated, the system evaluates the applicable structural constraints against the current state. This evaluation consults the fields, policies, and lineage records that travel with the objects themselves rather than relying on external state that may be stale, unavailable, or compromised.

The outcome of each evaluation is recorded in an append-only lineage structure. This record is cryptographically committed, ensuring that the complete history of decisions, transitions, and state changes remains auditable and tamper-evident. No evaluation outcome can be retroactively altered without breaking the cryptographic chain.

Because the evaluation logic and the data it operates on travel together, the mechanism functions identically across network partitions, substrate migrations, and administrative boundaries. There is no central evaluation point that must be available for the system to operate correctly.

What It Enables

With dynamic routing protocol (drp) as an architectural primitive, systems built on this foundation can operate autonomously while maintaining the structural guarantees that centralized architectures achieve through oversight. The capability is not a tradeoff between autonomy and governance but a resolution of the apparent conflict between them.

This enables deployment across centralized cloud infrastructure, federated multi-party environments, fully decentralized networks, and edge installations with intermittent connectivity. The structural guarantees hold regardless of deployment topology because they are properties of the objects and protocols themselves, not properties of the infrastructure that hosts them.

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

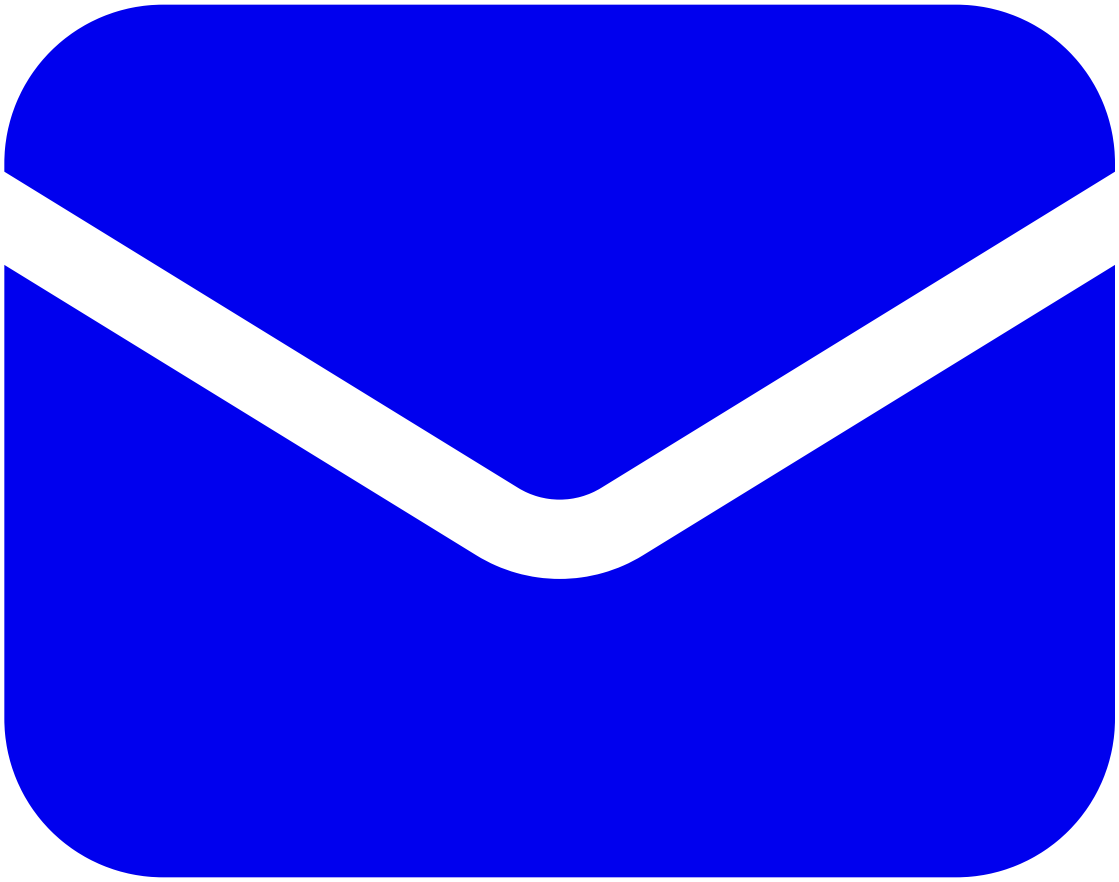
Legal

Subject to one or more pending U.S. and international patent applications, see Patents for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see Licensing. Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See Legal for terms and conditions.

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