# Module 10 – Anonymous Routing & Mesh Integrity Control

Module ID: COMM-MESH-010

Version: 4.1 (Revised CTO Edition)

Layer: Communication Control Layer

Status: RELEASE

Dependencies: Module 00, Module 09

## 0. Purpose & Enforcement Point

This module defines the anonymized routing and mesh communication integrity enforcement layer for MaxOneOpen v4.1. It ensures that all messages are transmitted across a validated node mesh without exposing identity paths or allowing pattern-based deanonymization. Routing is capsule-controlled, TTL-limited, and trust-filtered across all hops.

## 1. Routing Structure, Hop Control & Invocation Flow

Anonymous routing is invoked using `MESH\_ROUTE\_SEND()` which accepts:  
- `from\_identity\_token`  
- `target\_service\_id`  
- `payload`, `scope\_class`, `TTL`, `relay\_options`  
Routing is handled by the Mesh Relay Engine (MRE), which:  
- selects relay path based on trust zone separation  
- applies time decay and integrity checks at each hop  
- obfuscates previous hop using randomized capsule header chains

## 2. Mesh Capsule Format, Integrity Anchors & TTL Control

Each routed message is encapsulated in a `Mesh Capsule (MCAP)`:  
`{ capsule\_id, current\_hop\_id, TTL\_remaining, scope\_class, payload\_hash, previous\_hop\_mask, timestamp }`  
Each hop produces a `Hop Trace Capsule (HTC)` documenting validation and trust passage.  
Capsule chains are anchored into the LedgerSync chain for full traceability and tamper detection.

## 3. Anti-Deanonymization Safeguards & Trust Filtering

To preserve communication anonymity and trust alignment:  
- origin identity is never exposed in capsule header  
- routing patterns are randomized within permitted mesh zones  
- trust zones (0–5) define permissible hop scope  
- rule filters (from Module 04) define relay exclusion zones  
- message TTL ensures bounded propagation and replay rejection

## 4. Violation Triggers, Replay Defense & Forensic Records

Routing violations include:  
- TTL exhaustion → `TTL Violation Capsule (TVC)`  
- trust zone crossing without authority → `Trust Breach Capsule (TBC)`  
- header tampering → `Mesh Integrity Violation Capsule (MIVC)`  
All forensic records are capsule-bound and traceable to the initiating Mesh Capsule ID.

## 5. Intermodular Bindings & Routing Enforcement Chain

This module interacts with:  
- Module 09 (Twin Messaging) as pre-routing gate  
- Module 04 (MaxReg) to apply routing rules  
- Module 12 (Trust Enforcement) to constrain hop eligibility  
- Module 13 (LedgerSync) for route chain anchoring  
- Module 14 (Audit) to reconstruct and validate route integrity

## CTO Validation Matrix

Module 10 (CTO Edition) guarantees the following verifiable conditions:  
- All routed messages are encapsulated in anonymous mesh capsules: YES  
- Hop chains are trust-filtered, TTL-bound, and integrity-anchored: YES  
- Mesh routing patterns are obfuscated and randomized: YES  
- Violations (TTL, trust breach, tampering) trigger capsule audits: YES  
- Route history is cryptographically traceable and forensically complete: YES