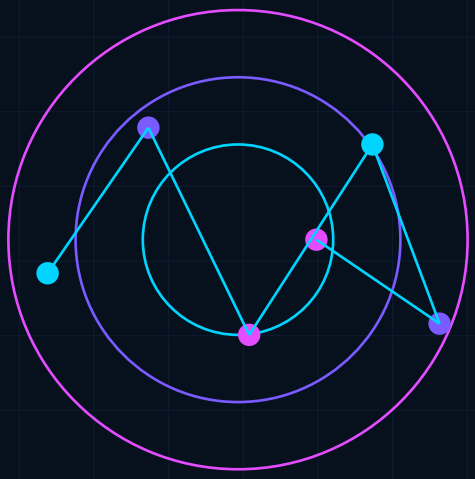
POST-QUANTUM MIGRATION

Post-Quantum Network Migration (Hybrid TLS realities)

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-008	A	BEGIN CONTROLLED MIGRATION	ACTIVE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2026-12-16

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **A**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **5 registered authorities**

NIST Post-Quantum Cryptography Project; Standard; FIPS 204 - Module-Lattice-Based Digital Signature Standard

FRESHNESS — **ACTIVE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **BEGIN CONTROLLED MIGRATION**

Begin cryptographic inventory, agility, hybrid interoperability testing, and migration sequencing now. Do not claim quantum safety from algorithm substitution alone.

REVIEW TRIGGER — **2026-12-16**

Scheduled at 90 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

NIST Post-Quantum Cryptography Project

https://csrc.nist.gov/projects/post-quantum-cryptography

AUTHORITY 02

Standard

https://csrc.nist.gov/pubs/fips/203/final

AUTHORITY 03

FIPS 204 - Module-Lattice-Based Digital Signature Standard

https://csrc.nist.gov/pubs/fips/204/final

AUTHORITY 04

FIPS 205 - Stateless Hash-Based Digital Signature Standard

https://csrc.nist.gov/pubs/fips/205/final

2026-09-17 FRESHNESS DELTA

NIST FIPS 203, 204, and 205 remain final PQC standards; migration guidance remains active and event-driven review is required.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

LIMITATIONS / CONFLICTS / REPRODUCIBILITY

Evidence Must Survive Contact With Reality

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.
- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.
- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.
- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

ADOPTION / VALIDATION / REVIEW

Decision Gate and Validation Plan

ADOPTION POSTURE

BEGIN CONTROLLED MIGRATION

Begin cryptographic inventory, agility, hybrid interoperability testing, and migration sequencing now. Do not claim quantum safety from algorithm substitution alone.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2026-12-16 (90-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-008 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Network architects, security engineers, and platform teams executing the Post-Quantum Cryptography (PQC) migration of TLS/IPsec fabrics, VPNs, and internal service meshes Companion Standards: MYTHOS-SEC-0001 (Post-Quantum Cryptography & Crypto-Agility), MYTHOS-NET-0010 (Routing, DNS & IPAM), MYTHOS-NET-0008 (OSI Troubleshooting), MYTHOS-CLD-0001 (Multi-Cloud Architecture)

The migration to Post-Quantum Cryptography (PQC) is not a software update; it is a network architecture crisis. Organizations recognize the threat of Harvest Now, Decrypt Later (HNDL) and mandate the transition to NIST FIPS 203 (ML-KEM). However, they attempt to drop PQC algorithms into existing TLS 1.3 handshakes without understanding the physics of the network.

The reality of Hybrid TLS—where a classical algorithm (X25519) is paired with a PQC algorithm (ML-KEM-768) to hedge against cryptanalytic breaks—is that it drastically inflates the size of the cryptographic key exchange. A standard TLS ClientHello that easily fits into a single 1500-byte MTU packet suddenly balloons to over 1600 bytes.

This research note defines the hard realities of Post-Quantum network migration. It exposes how PQC key inflation shatters legacy MTU boundaries, causes middlebox black holes, and introduces new downgrade attack vectors. Executing a PQC migration without addressing Layer 2/3 MSS clamping and middlebox inspection boundaries does not increase security; it breaks the network.

To understand the migration crisis, we must map the mathematical difference between classical and PQC key exchanges.

- Classical Key Exchange (ECDHE): Uses elliptic curve cryptography (e.g., X25519). The public key is tiny—exactly 32 bytes. The entire TLS 1.3 `ClientHello` (including certificates and extensions) typically consumes ~500 to 800 bytes, easily fitting within a single standard Ethernet frame.
- Post-Quantum Key Exchange (ML-KEM): Uses lattice-based cryptography (e.g., ML-KEM-768). The public key is massive—1,184 bytes. The ciphertext is equally massive.
- The Hybrid Bind: To ensure safety, modern systems (like Google Chrome or AWS Post-Quantum TLS) combine both. The `key_share` extension in the `ClientHello` contains both the 32-byte X25519 key and the 1,184-byte ML-KEM key.

The resulting `ClientHello` is so large that it cannot be transmitted in a single TCP segment over a standard 1500-byte Maximum Transmission Unit (MTU) link. It must be fragmented across multiple TCP packets.

When the TLS handshake breaks out of a single packet, it collides with the physical and logical realities of the internet and enterprise networks.

2.1 The MTU/MSS Black Hole

The most common failure mode in PQC migration is the TCP Maximum Segment Size (MSS) black hole.

- The Mechanic: The client sends a 1600-byte `ClientHello`. The network layer fragments this into two TCP segments (e.g., 1480 bytes and 120 bytes).

- The Flaw: Many internet paths, VPN concentrators, and cloud overlay networks (like GRE or IPsec tunnels) reduce the available MTU. If the path MTU is lower than expected, and ICMP "Fragmentation Needed" packets are blocked by a firewall, the TCP handshake completes but the TLS handshake hangs forever. The connection dies silently.
- The Impact: Users cannot access the application. The failure is intermittent, depending on the specific ISP or VPN path, making it nearly impossible to troubleshoot with standard tools.

2.2 Middlebox Blindness and SSL Inspection

Enterprise networks rely heavily on Middleboxes—Firewalls, Intrusion Prevention Systems (IPS), and Secure Web Gateways that perform deep packet inspection (DPI) on TLS traffic.

- The Mechanic: Middleboxes are programmed to inspect the first packet of a TLS connection (the `ClientHello`) to identify the SNI (Server Name Indication) and enforce policy.
- The Flaw: When the `ClientHello` is fragmented across two TCP segments, older or poorly configured middleboxes only inspect the first segment. They fail to see the SNI or the PQC extensions in the second segment. They classify the traffic as "unknown" or "malformed" and silently drop the connection.
- The Impact: Internal applications fail when PQC is enabled, but only when traffic traverses specific datacenter firewalls.

2.3 Performance and Latency Overhead

PQC algorithms (ML-KEM) are computationally fast, but the sheer volume of data being transmitted impacts latency.

- The Mechanic: Transmitting 1,184 bytes over a high-latency, low-bandwidth IoT or satellite link takes significantly longer than 32 bytes.
- The Impact: On constrained networks, the TLS handshake latency increases by 20-50ms. For time-sensitive protocols (like DNS over TLS or financial trading APIs), this latency spike is unacceptable.

The fragmentation of the `ClientHello` introduces a new, dangerous attack surface: the Protocol Downgrade.

3.1 The Downgrade Stripping Attack

An attacker (or a compromised middlebox) intercepts the fragmented TCP stream. They intentionally drop the second TCP segment containing the ML-KEM `key_share` extension.

- The server receives an incomplete `ClientHello`.
- If the server is configured for "opportunistic" PQC, it falls back to classical X25519 to maintain connectivity.
- The connection is established, but it is no longer quantum-resistant. The attacker continues to harvest the traffic via HNDL, defeating the entire purpose of the migration.

3.2 The Middleman DoS

Because PQC handshakes consume more bandwidth, an attacker can amplify a Denial of Service (DoS) attack. By sending a flood of PQC `ClientHello` requests, the attacker forces the server to process massive cryptographic payloads and fragments, exhausting CPU and memory resources faster than a classical TLS flood.

Executing a PQC migration without addressing the network layer is architectural malpractice. The Mythos standard mandates a holistic approach.

4.1 Aggressive TCP MSS Clamping

Before enabling PQC on any internal or external service, the network edge MUST be configured to enforce TCP MSS Clamping.

- Edge routers and firewalls MUST intercept TCP SYN packets and rewrite the MSS option to a safe value (e.g., 1200 bytes).
- This forces the client and server to send smaller TCP segments from the start, ensuring the massive `ClientHello` fits within the MTU boundaries without relying on ICMP.

4.2 The "Client Hello Splitting" Extension

Modern TLS implementations MUST utilize the `TLS Client Hello Splitting` extension (or similar mechanisms) that intentionally splits the `ClientHello` into two records at the TLS layer, rather than relying on the TCP layer to fragment it.

- This allows middleboxes to easily reassemble the TLS record without relying on TCP segment reassembly, bypassing the middlebox blindness problem.

4.3 Strict Downgrade Resistance

PQC MUST NOT be deployed in an "opportunistic" mode.

- If a client offers ML-KEM, and the server supports it, the connection MUST use ML-KEM.
- If the `key_share` extension is stripped or dropped, the handshake MUST abort, rather than falling back to X25519.
- While this reduces compatibility, it guarantees that HNDL is actually prevented.

4.4 Crypto-Agility (Algorithm Registries)

The network MUST be governed by an agile algorithm registry. If ML-KEM-768 is found to be flawed, the registry MUST be updated to switch to ML-KEM-1024 or SLH-DSA without requiring code changes or network re-architecture.

The Post-Quantum migration is not just a cryptographic upgrade; it is a fundamental shift in the physics of the network. The massive key sizes of lattice-based cryptography shatter the assumptions of single-packet TLS handshakes. By proactively enforcing MSS clamping, updating middlebox inspection logic, and mandating strict downgrade resistance, organizations can traverse the Hybrid TLS transition without sacrificing availability or security.

```
A 32-byte key fits in a packet; a 1,184-byte key shatters it.
A fragmented handshake is a middlebox blind spot.
A silent fallback is a cryptographic surrender.

Cryptography may be mathematically sound; the network must be physically prepared.

> Algorithms may be quantum-resistant.
> The network must be MTU-prepared.
```

End of Research Note RES-008

9. Source Register

Source	Authority and Status	Freshness Control
NIST Post-Quantum Cryptography Project https://csrc.nist.gov/projects/post-quantum-cryptography	Primary government standards program Active Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIPS 204 - Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIPS 205 - Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
IETF TLS Hybrid Key Exchange Design https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/	Primary standards draft Internet-Draft - volatile Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-008_Post_Quantum_Network_Migration_Hybrid_TLS_realities.md
Original source words	1314
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	90 days or event-driven trigger, whichever occurs first