Nyx Protocol v1.0 — Complete Feature Specification

> **Status: Draft-Complete (includes planned features)**

Feature Differences (v0.1 → v1.0)

Category	v0.1	v1.0 Extensions
Cryptography	X25519, Kyber optional	PQ-Only mode (Kyber/BIKE), Hybrid DH, HPKE support
Routing	Fixed 5-hop Mix	Dynamic hop count (3–7), Multipath concurrent communication, Latency-aware routing (LARMix++)
Transport	Single UDP	UDP + QUIC DATAGRAM, TCP fallback, IPv6 Teredo built-in
FEC	RS(255,223)	RaptorQ, adaptive redundancy
Security	Basic replay protection	VDF-based cMix batch, post-compromise recovery
Extensions	SETTINGS only	Capability Negotiation via CBOR, Plugin Frames
Monitoring	Prometheus	OpenTelemetry tracing, push/pull both
Mobile	-	Low Power Mode (Adaptive cover traffic rate)

---

1. Protocol Combinator (Plugin Framework)

- New Frame Type 0x50–0x5F reserved for "Plugin".
- CBOR header `{id:u32, flags:u8, data:bytes}`.
- Plugin handshake: SETTINGS `PLUGIN_REQUIRED` advertising.

2. Multipath Data Plane

- `path_id` (uint8) per CID. Added to packet header.
- Transmission scheduler: Weighted Round Robin of paths, weight = inverse RTT.
- Dynamic reordering buffer size (RTT diff + jitter *2).

3. Hybrid Post-Quantum Handshake

```
<- s
-> e, ee_dh25519, ee_kyber, s, ss
<- se_dh25519, se_kyber, es, ee_dh25519, ee_kyber
```

- Secret = HKDF-Extract(SHA-512, concat(dh25519, kyber)).

4. cMix Integration

- Optional `mode=cmix` with batch = 100, VDF delay 100ms.
- Mix nodes publish proofs via RSA accumulator.

5. Adaptive Cover Traffic

- Target utilization U∈[0.2,0.6]. Measured in 1s window→λ adjustment.

6. Low Power Mode (Mobile)

- Screen-Off detection sets `cover_ratio`=0.1, keepalive 60s.
- Push notification path: FCM / APNS WebPush over Nyx Gateway.

7. Extended Packet Format

Byte	Name	Description
0–11	CID	Connection ID
12	Type(2) + Flags(6)	
13	PathID (8)	
14–15	Length	
16–...	Payload	

8. Capability Negotiation

- Extension list CBOR array in first CRYPTO frame.
- Unsupported Required → CLOSE 0x07 (UNSUPPORTED_CAP).

9. Telemetry Schema (OTLP)

- span name = "nyx.stream.send" attr: path_id, cid.

10. Compliance Levels

Level	Required Features	Description
Core	v0.1 set	Minimum compatibility
Plus	Multipath, Hybrid PQ	Default recommended
Full	cMix, Plugin, LowPower	All features

Implementation Architecture

Core Components

Cryptographic Layer (`nyx-crypto`)

- **Noise Protocol**: Complete Noise_Nyx handshake implementation
- **HKDF**: Key derivation functions with misuse-resistant label semantics
- **AEAD**: Authenticated encryption with associated data
- **Keystore**: Secure key management system with zeroization
- **Post-Quantum**: Optional Kyber1024 and BIKE support
- **HPKE**: RFC 9180 compliant Hybrid Public Key Encryption
- **PCR Rekey**: Post-Compromise Recovery with forward secrecy

Stream Layer (`nyx-stream`)

- **Frame Processing**: Multiple frame types (Data, ACK, Management)
- **Congestion Control**: Adaptive congestion control algorithms
- **Multipath Support**: Concurrent communication over multiple paths
- **Reordering Buffer**: Packet sequence restoration
- **Plugin System**: Dynamic feature extension framework
- **Capability Negotiation**: CBOR-based feature negotiation
- **Management Frames**: Ping/Pong, Close, Settings, Path Challenge/Response
- **Internationalization**: Multi-language string frames
- **HPKE Rekey**: Periodic session key renewal

Mix Routing (`nyx-mix`)

- **Weighted Path Building**: Latency and bandwidth-aware route selection
- **Cover Traffic**: Poisson-distributed dummy traffic generation
- **Adaptive Cover Traffic**: Dynamic rate adjustment based on utilization
- **cMix Integration**: Batch processing with VDF delays
- **LARMix**: Latency-aware routing protocols
- **Anonymity Evaluation**: Anonymous set analysis capabilities

Transport Layer (`nyx-transport`)

- **UDP Pool**: Efficient socket management with SO_REUSEPORT
- **ICE-lite**: Basic NAT traversal capabilities
- **Teredo**: IPv6 over IPv4 tunneling support
- **QUIC Extensions**: QUIC DATAGRAM support (feature-gated)
- **TCP Fallback**: TCP encapsulation when QUIC unavailable
- **Path Validation**: Connection path verification

Forward Error Correction (`nyx-fec`)

- **Reed-Solomon**: Default 10+3 configuration (30% overhead)
- **RaptorQ**: Adaptive rateless coding
- **Timing Obfuscation**: Packet transmission timing concealment
- **Padding**: Fixed-size packets (1280 bytes)

Control Plane (`nyx-control`)

- **DHT**: Kademlia distributed hash table

- **Push Notifications**: FCM/APNS integration
- **Probing**: Network quality measurement
- **Configuration Sync**: Distributed configuration management

Daemon (`nyx-daemon`)

- **gRPC API**: Comprehensive control interface
- **Stream Management**: Connection lifecycle management
- **Metrics Collection**: Real-time performance monitoring
- **Path Building**: Geographic diversity-aware routing
- **Session Management**: Connection ID (CID) based sessions
- **Health Monitoring**: System health checks
- **Event System**: Real-time event distribution

CLI (`nyx-cli`)

- **Connection**: Anonymous connection to targets
- **Status Display**: Detailed daemon status reporting
- **Benchmarking**: Performance measurement capabilities
- **Internationalization**: Japanese, English, Chinese support
- **Interactive Mode**: Interactive operation support

Core Library (`nyx-core`)

- **Configuration**: TOML configuration file processing
- **Error Handling**: Unified error types
- **Type Definitions**: Common data types (NodeId, etc.)
- **Sandboxing**: Linux seccomp, OpenBSD pledge/unveil
- **Internationalization**: i18n string management
- **Mobile Support**: Battery efficiency optimizations
- **Push Notifications**: Mobile push integration
- **Capability Management**: Feature flag system
- **Compliance**: Regulatory compliance levels

Security Features

Memory Safety

- **Rust Implementation**: Memory-safe implementation throughout
- **Unsafe Code Forbidden**: `#![forbid(unsafe_code)]` in all crates
- **Zeroization**: Automatic key material cleanup

Sandboxing

- **Linux**: seccomp-bpf system call filtering
- **OpenBSD**: pledge and unveil restrictions
- **Windows**: Process isolation (planned)

Cryptographic Security

- **Post-Quantum Ready**: Kyber1024 and BIKE support
- **Perfect Forward Secrecy**: Ephemeral key exchanges
- **Post-Compromise Recovery**: Automatic key rotation

Performance Optimizations

Multipath Communication

- **Weighted Round Robin**: Path selection based on RTT and bandwidth
- **Dynamic Load Balancing**: Adaptive traffic distribution
- **Congestion Awareness**: Responsive to network conditions

Efficient Transport

- **Socket Reuse**: SO_REUSEPORT for improved performance
- **Zero-Copy**: Minimized memory allocations
- **Async I/O**: Tokio-based asynchronous operations

Testing Framework

Comprehensive Test Suite

- **Unit Tests**: Individual component testing
- **Integration Tests**: Cross-crate interaction testing
- **Conformance Tests**: Protocol specification compliance
- **Load Testing**: High-load environment validation
- **Security Testing**: Cryptographic implementation verification

Deployment and Operations

Configuration Management

- **TOML Configuration**: Human-readable configuration files
- **Hot Reload**: Runtime configuration updates
- **Environment Variables**: Container-friendly configuration

Monitoring and Observability

- **OpenTelemetry**: Distributed tracing support
- **Prometheus Metrics**: Performance and health metrics
- **Structured Logging**: JSON-formatted log output
- **Health Checks**: Comprehensive system health monitoring

Platform Support

- **Cross-Platform**: Windows, Linux, macOS support
- **Mobile Optimization**: Android and iOS considerations

- **Container Ready**: Docker and Kubernetes deployment

This specification represents the current implementation state and planned extensions for the Nyx Protocol v1.0, providing a comprehensive anonymity network with modern cryptographic primitives and high-performance networking capabilities.