MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

Routing, DNS, DHCP, and IPAM Standard

Defines routing architecture, naming, addressing, DDI, policy, operations, and assurance.

PERMANENT DOCUMENT ID
MYTHOS-NET-0010

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
6 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Routing, DNS, DHCP, and IPAM Standard

Defines routing architecture, naming, addressing, DDI, policy, operations, and assurance.

DOCUMENT ID
MYTHOS-NET-0010

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

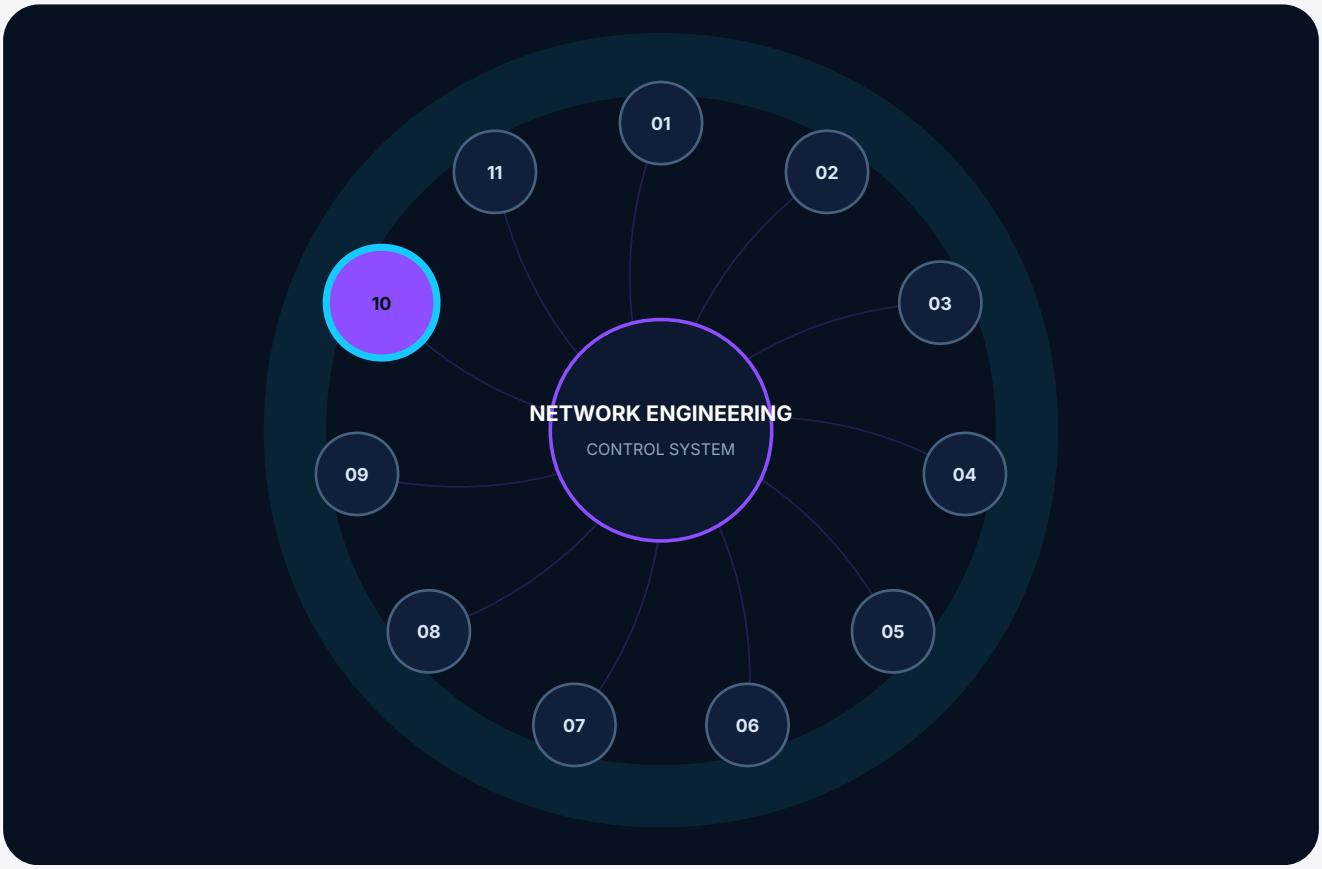
CLASSIFICATION
Public

6	6	4	1
ATOMIC CRITERIA	CAPABILITY FAMILIES	ASSESSMENT PROFILES	PERMANENT IDENTITY

Publication doctrine. This standard establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, and formal revision history.

DOMAIN CONTROL SYSTEM

MYTHOS-NET-0010 inside the network engineering standard constellation



Connected assurance

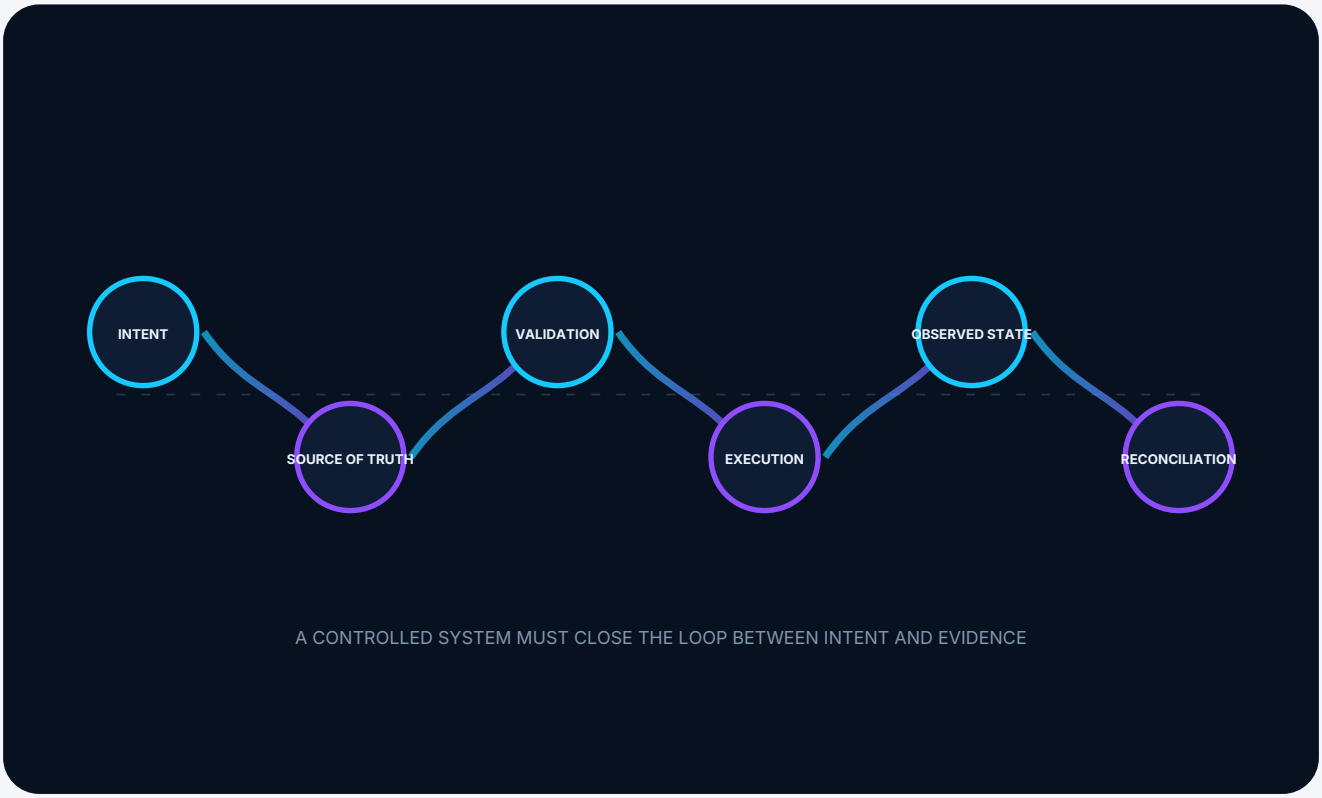
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

Specialization rule

Companion standards may add precision, but they cannot silently weaken this publication's requirements.

CLOSED-LOOP ARCHITECTURE

Intent becomes trustworthy only when observed state returns as evidence



State separation

Desired, approved, deployed, observed, historical, and simulated states must remain distinguishable.

Recoverable change

Material change requires validation, authorization, monitoring, containment, and a credible recovery path.

EVALUATION TOPOLOGY

The capability families and atomic criteria of MYTHOS-NET-0010

Capability families

Families expose the major engineering surfaces and preserve the source weighting model.

Atomic criteria

Each criterion carries a question, maturity spectrum, evidence expectations, assessment method, and operational signals.

NAVIGATION

Contents

ENGINEERING DOCTRINE

0. Executive Mandate

The architecture of core network services has failed.

Organizations attempt to manage millions of IP addresses across multi-cloud and on-premises environments using static Excel spreadsheets. They accept BGP routes from transit providers based on "trust" rather than cryptographic validation, leaving the global routing table vulnerable to hijacking. They expose internal DNS queries in plaintext, allowing attackers to map network topologies and exfiltrate data via DNS tunneling.

This standard exists because:

1. **Spreadsheets are Not IPAM:** Tracking IP allocations in a spreadsheet guarantees IP conflicts, orphaned addresses, and broken automation. IPAM MUST be a dynamic, API-first system integrated with DNS and DHCP (DDI), serving as the absolute Source of Truth for network intent.
2. **BGP is an Unauthenticated Anarchy:** The default global routing infrastructure assumes all participants are honest. Without RPKI (Resource Public Key Infrastructure) and Route Origin Validation (ROV), any attacker can hijack an IP prefix and reroute global traffic. Production routing MUST cryptographically validate routes.
3. **DNS is an Attack Surface, Not a Phonebook:** Plaintext DNS allows ISPs and attackers to inspect, block, or poison name resolutions. Furthermore, internal DNS queries reveal topological secrets. Systems MUST enforce DNSSEC for data integrity and DNS over HTTPS/TLS (DoH/DoT) for transport privacy.
4. **Manual DHCP is a Bottleneck:** In modern, ephemeral infrastructure, IP allocation must happen at machine speed. DDI MUST be fully automated, integrating with cloud providers and Kubernetes to allocate, reserve, and reclaim addresses without human intervention.

This document establishes the **Mythos Routing, DNS & IPAM Standard (MRDIS)**, a comprehensive, evidence-based methodology for evaluating core network services against cryptographic routing validation, zero-trust name resolution, and automated address lifecycle management.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- DDI (DNS, DHCP, IPAM) platforms (BlueCat, Infoblox, NetBox, Nautobot)
- Routing protocols and architectures (BGP, OSPF, IS-IS, MPLS, VXLAN/EVPN)
- Route security (RPKI, Route Origin Validation, BGPsec, MANRS)
- DNS architecture (Split-horizon, DNSSEC, DoH, DoT, DNS tunneling prevention)
- DHCP automation and IP lifecycle management (allocation, reclamation, conflict detection)

1.2 Out of Scope

- Physical layer cabling and topology (covered in MYTHOS-NET-0009)
- High-level network design and intent (covered in MYTHOS-NET-0001)
- Zero-trust network access (ZTNA) and microsegmentation policy (covered in MYTHOS-SEC-0007)

1.3 Audience

- Network engineers and architects designing core infrastructure
- Cloud and platform engineers managing IP allocation at scale
- Security engineers evaluating DNS attack surfaces and route hijacking
- DevSecOps teams automating network configuration
- Standards bodies seeking a reference DDI and routing methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Core Service Dimensions

Dimension	Definition
DDI	The convergence of DNS, DHCP, and IPAM into a single, unified management platform.
RPKI (Resource Public Key Infrastructure)	A cryptographic framework that binds IP address prefixes to their rightful Autonomous System (ASN), allowing routers to validate BGP routes.
Route Origin Validation (ROV)	The process of a BGP router dropping routes that do not match RPKI records, preventing prefix hijacking.
Split-Horizon DNS	An architecture where internal and external clients receive different IP address responses for the same domain name, hiding internal topology.
DNSSEC	A suite of cryptographic extensions to DNS that authenticates the origin of DNS data, verifying it has not been modified in transit.
IPAM Source of Truth	The principle that the IPAM system is the sole authority for IP allocation; no IP is assigned via CLI or cloud console without IPAM API approval.

2.2 The Core Services Doctrine

> A spreadsheet is not a source of truth. An unvalidated BGP route is a hijack. A plaintext DNS query is a public broadcast. If the IP lifecycle is not automated, the network cannot scale.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; spreadsheets for IPAM, unvalidated BGP, plaintext DNS
1	Basic DDI exists, but manual processes and no RPKI enforcement
2	Functional routing and DNS, but lacks cryptographic validation or automation
3	Solid production performance; API-driven DDI, RPKI/ROV enforced, DNSSEC, split-horizon DNS
4	Strong performance; BGPsec, DoH/DoT internally, automated IP reclamation
5	Best-in-class; sets the standard for mathematically verified, zero-trust core services

Weighting

Category	Weight	Rationale
IPAM & DDI Automation	25%	Manual IP tracking breaks at cloud scale and causes conflicts
BGP & Routing Security (RPKI)	20%	Unvalidated routes allow global traffic hijacking
DNS Security & Privacy	20%	Plaintext DNS is easily spoofed and mined for intelligence
DHCP & Address Lifecycle	15%	Ephemeral compute requires sub-second, automated allocation
High Availability & Resilience	10%	Core services are single points of failure; must be highly available
Observability & Drift Detection	10%	IPAM must reconcile with actual network state

Total: 100%

A system MUST score at least 3.0 in IPAM Automation and BGP/Routing Security to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

Capability claims are bounded by evidence, context, and reproducible assessment.

6 atomic criteria across 6 capability families define the evaluation surface of this standard.

4.1 / CAPABILITY FAMILY

IPAM and DDI Automation

SOURCE WEIGHT 25%

4.1.1
Address Management Authority

MYTHOS-NET-0010-EVAL-4.1.1

Address Management Authority

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
IPAM and DDI Automation	4.1.1	25%	Evidence-led

Is the IPAM system the absolute, automated Source of Truth for all IP addresses?

0
IP addresses tracked in spreadsheets; manual CLI configuration on devices

1
Basic IPAM tool used, but requires manual sync with DNS/DHCP

2
Integrated DDI platform, but lacks API integration with cloud/Kubernetes

3
API-first DDI: all IP allocations (on-prem, cloud, k8s) automated via API; zero manual CLI allocation

4
Automated IP reclamation: DDI detects orphaned IPs and reclaims them dynamically

5
Leading authority: formally verified IP lifecycle, zero IP conflicts possible, cryptographic attestation of allocations

ENGINEERING INTERPRETATION

This criterion evaluates whether address management authority is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- source-of-truth objects, Git history, observed-state snapshots, and reconciliation evidence
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. introduce controlled drift and verify detection, adjudication, and restoration
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- multiple authorities, silent manual changes, stale inventory, and destructive auto-remediation
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- drift detection time
- reconciliation success
- unowned object count
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.2 / CAPABILITY FAMILY

BGP and Routing Security (RPKI)

SOURCE WEIGHT 20%

4.2.1
Route Validation

MYTHOS-NET-0010-EVAL-4.2.1

Route Validation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
BGP and Routing Security (RPKI)	**4.2.1**	**20%**	**Evidence-led**

Is the global routing table cryptographically protected against hijacking?

0
BGP operates on pure trust; no RPKI; accepts any route from peers

1
RPKI signed on outbound, but no inbound Route Origin Validation (ROV)

2
ROV enabled, but in "monitoring" mode (does not drop invalid routes)

3
ROV enforced in "dropping" mode; rejects unauthorized BGP routes

4
BGPsec implemented cryptographically validating the entire AS_PATH

5
Leading security: formally verified routing boundaries, zero ability to inject unauthorized prefixes, full MANRS compliance

ENGINEERING INTERPRETATION

This criterion evaluates whether route validation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- routing policy, RIB/FIB snapshots, adjacency state, and path-analysis output
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. simulate route withdrawal, policy conflict, convergence, and rollback
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- route leaks, asymmetric paths, stale advertisements, and unbounded convergence
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- route-policy compliance
- convergence time
- unexpected path count
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.3 / CAPABILITY FAMILY

DNS Security and Privacy

SOURCE WEIGHT 20%

4.3.1
Name Resolution Integrity

MYTHOS-NET-0010-EVAL-4.3.1

Name Resolution Integrity

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
DNS Security and Privacy	4.3.1	20%	Evidence-led

Are DNS queries protected against spoofing, interception, and surveillance?

0
Open recursive resolvers; plaintext DNS; no DNSSEC

1
Internal DNS servers, but queries sent in plaintext

2
DNSSEC implemented on authoritative zones, but not validated by resolvers

3
DNSSEC validated end-to-end; split-horizon DNS hiding internal topology

4
DoH/DoT (DNS over HTTPS/TLS) enforced for all internal and external queries

5
Leading integrity: formally verified cryptographic resolution, zero plaintext DNS, AI-driven DNS tunneling detection

ENGINEERING INTERPRETATION

This criterion evaluates whether name resolution integrity is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.4 / CAPABILITY FAMILY

DHCP and Address Lifecycle

SOURCE WEIGHT 15%

4.4.1
Dynamic Allocation

MYTHOS-NET-0010-EVAL-4.4.1

Dynamic Allocation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
DHCP and Address Lifecycle	**4.4.1**	**15%**	**Evidence-led**

How are addresses allocated to ephemeral and physical devices?

0
Static IP assignments; no DHCP

1
Basic DHCP server, but with finite scopes and manual management

2
DHCP integrated with IPAM, but lacks rapid reclamation

3
Dynamic DHCP with automated lease tracking and conflict detection (ARP ping)

4
Ephemeral compute integration: Kubernetes and cloud instances allocated via DHCP relay to centralized DDI

5
Leading lifecycle: formally verified lease boundaries, zero IP exhaustion risk, sub-millisecond allocation at scale

ENGINEERING INTERPRETATION

This criterion evaluates whether dynamic allocation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.5 / CAPABILITY FAMILY

High Availability and Resilience

SOURCE WEIGHT 10%

4.5.1
Core Service Uptime

MYTHOS-NET-0010-EVAL-4.5.1

Core Service Uptime

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
High Availability and Resilience	4.5.1	10%	Evidence-led

Can the DDI and routing infrastructure survive node failures?

0
Single DNS server; single router; no failover

1
Primary/backup DNS; basic router redundancy (VRRP)

2
Anycast DNS deployed; routing control planes redundant (NSF/GR)

3
Active-active DDI clusters across multiple datacenters; seamless failover

4
Multi-region routing autonomy; DDI survives region loss without caching delays

5
Leading resilience: formally verified zero-downtime failover, mathematical proof of continuous name resolution

ENGINEERING INTERPRETATION

This criterion evaluates whether core service uptime is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- routing policy, RIB/FIB snapshots, adjacency state, and path-analysis output
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. simulate route withdrawal, policy conflict, convergence, and rollback
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- route leaks, asymmetric paths, stale advertisements, and unbounded convergence
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- route-policy compliance
- convergence time
- unexpected path count
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.6 / CAPABILITY FAMILY

Observability and Drift Detection

SOURCE WEIGHT 10%

4.6.1
State Reconciliation

MYTHOS-NET-0010-EVAL-4.6.1

State Reconciliation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Observability and Drift Detection	**4.6.1**	**10%**	**Evidence-led**

Does the actual network state continuously match the IPAM Source of Truth?

0
No monitoring; IPAM drifts from actual device configurations

1
Periodic manual audits of IP allocations

2
Automated scanning (Nmap) compared against IPAM, but requires manual remediation

3
Continuous reconciliation: DDI pulls live state from routers/cloud APIs and alerts on drift

4
Automated drift remediation: unauthorized IP allocations are immediately quarantined or overwritten

5
Leading observability: formally verified state parity, policy-defined drift tolerance, real-time topological visualization

ENGINEERING INTERPRETATION

This criterion evaluates whether state reconciliation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- source-of-truth objects, Git history, observed-state snapshots, and reconciliation evidence
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. introduce controlled drift and verify detection, adjudication, and restoration
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- multiple authorities, silent manual changes, stale inventory, and destructive auto-remediation
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- drift detection time
- reconciliation success
- unowned object count
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

LIFECYCLE AND ASSURANCE

Part V. The Mythos Routing & DDI Suite (MRDIS)

Traditional benchmarks measure DHCP lease throughput. The MRDIS evaluates route hijacking resistance, DNS spoofing immunity, and IPAM automation.

5.1 Suite Composition

5.1.1 MRDIS-Routing

- **Prefix Hijack Simulation:** 100+ tests announcing unauthorized BGP routes to edge routers, verifying RPKI/ROV immediately drops them.
- **Route Leak Test:** 50+ tests simulating a transit provider leaking full tables, verifying route maps and max-prefix limits drop the leak.

5.1.2 MRDIS-DNS_IPAM

- **Cache Poisoning Test:** 100+ tests injecting spoofed DNS responses, verifying DNSSEC cryptographic validation rejects them.
- **Drift Injection:** 50+ tests manually configuring an IP on a switch interface without IPAM approval, verifying the system detects the drift and alerts/remediates.

5.2 Execution Protocol

PUBLICATION BOUNDARY

Candidate standard. Permanent identity. Evidence before authority.

Approval requires designated technical, security, legal, accessibility, and governance review with recorded findings and dispositions.