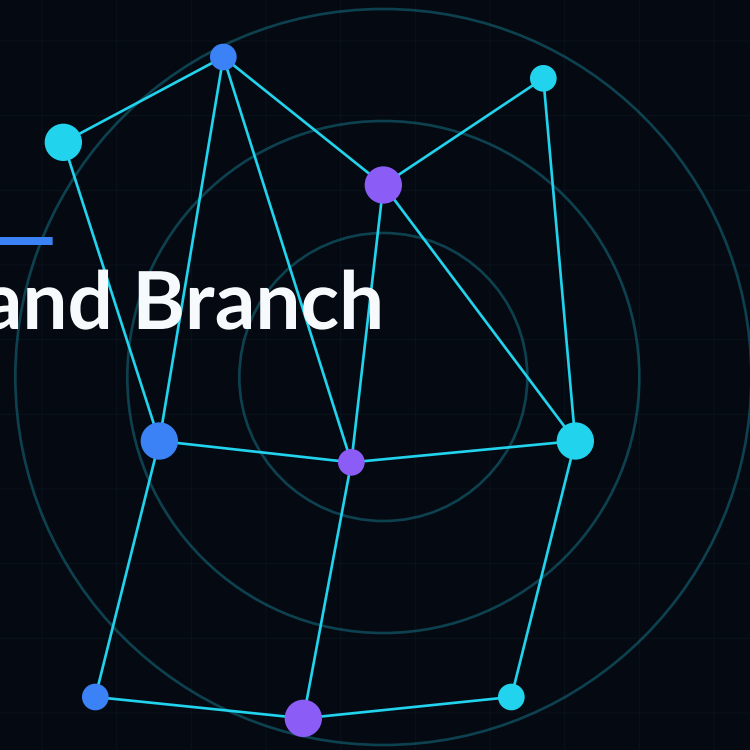




REFERENCE ARCHITECTURE / ENGINEERING STANDARDS LIBRARY

Enterprise Campus and Branch Network

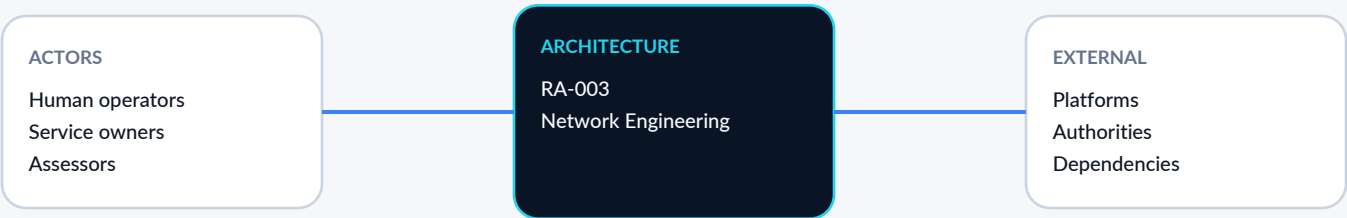


An identity-driven, observable, programmable campus, branch, wireless, WAN, and security architecture with explicit source of truth and change assurance.

Architecture identity and operating position

ARCHITECTURE SET Canonical Set	DOMAIN Network Engineering	LAYERS 6	COMPONENTS 6	ACCEPTANCE 18	DEPENDENCIES 0
--	-------------------------------	--------------------	------------------------	-------------------------	--------------------------

SYSTEM CONTEXT



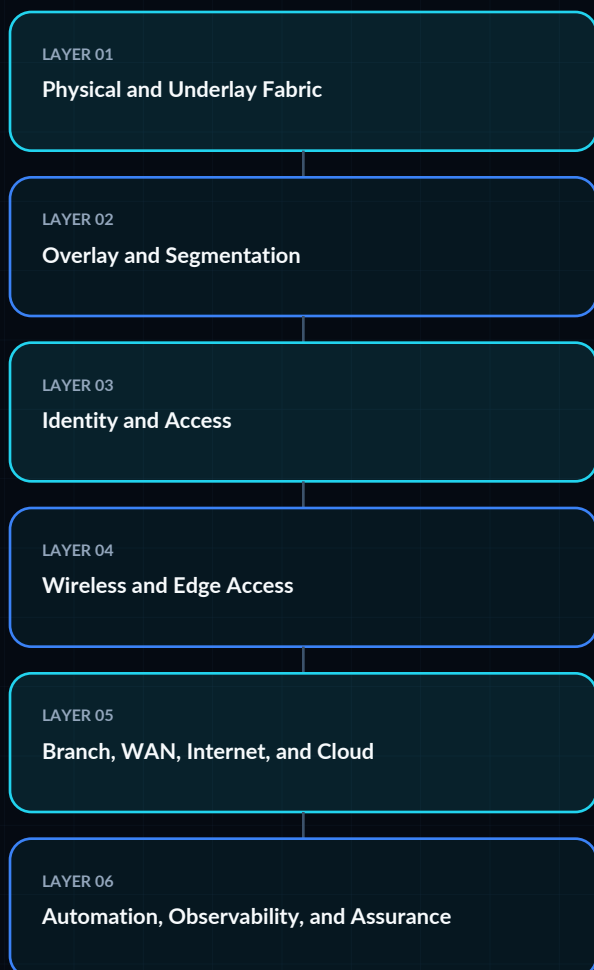
EXECUTIVE OUTCOMES

- 1 Deliver predictable user, device, application, and site connectivity.
- 2 Bind access to identity, posture, role, and policy rather than physical location alone.
- 3 Reduce failure domains through routed design, resilient services, and explicit local survivability.
- 4 Operate the network from authoritative intent, telemetry, validation, and controlled change.

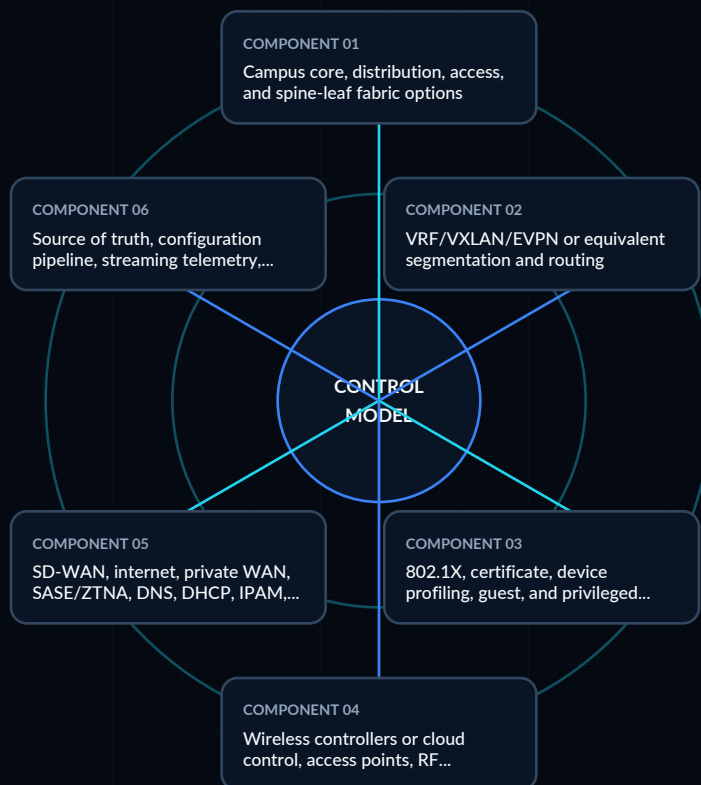
ARCHITECTURE DOCTRINE

Interpret the architecture as a bounded operating model: explicit ownership, least authority, separable desired/runtime/observed/evidence state, safe degradation, reversible change, measurable outcomes, and evidence-backed acceptance.

Layered architecture and component model

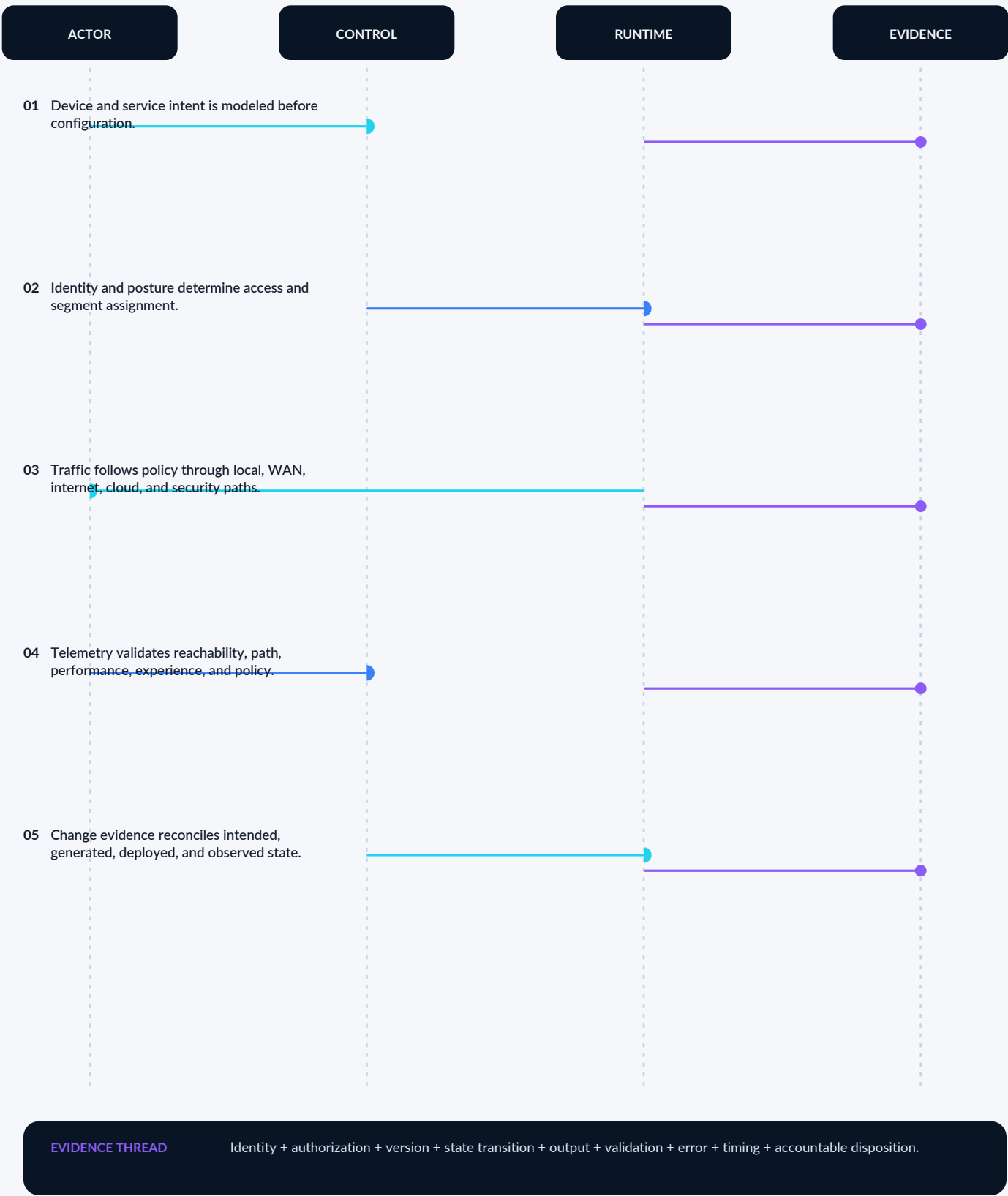


CORE COMPONENTS



Each layer and component owns an explicit interface, state model, authority boundary, failure behavior, telemetry contract, recovery path, and evidence obligation.

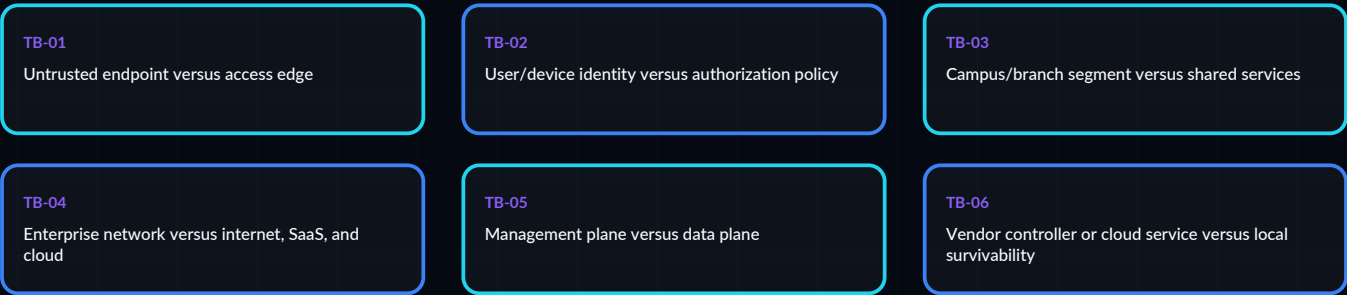
Primary sequence and control flow



State, data, authority, and trust flow

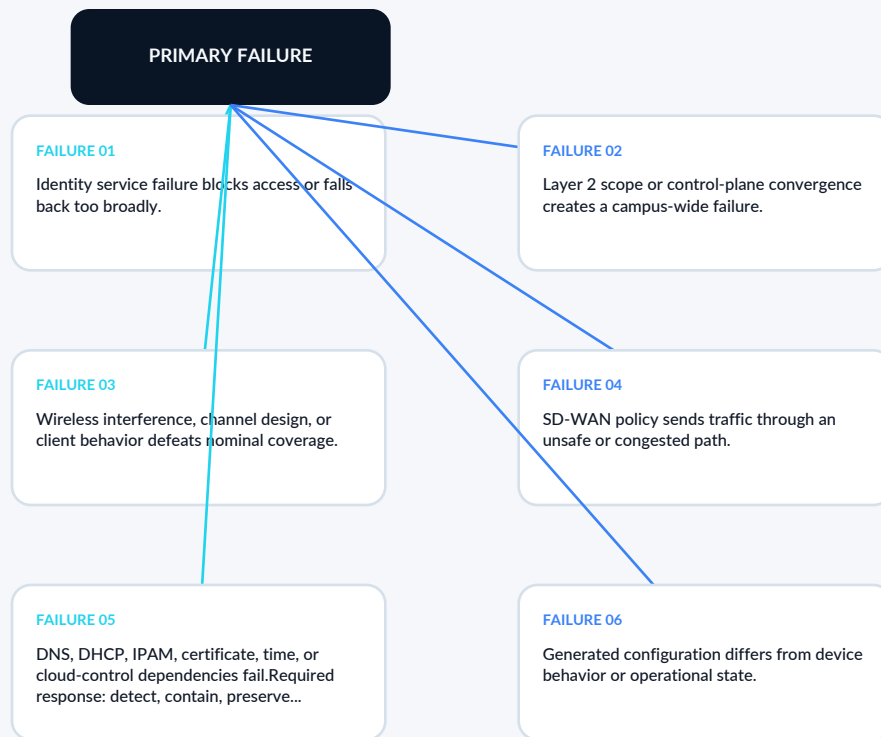


TRUST BOUNDARY REGISTER



Failure propagation and observability

FAILURE PATHS



OBSERVABILITY STACK

OUTCOME

User / mission result

SERVICE

SLOs / availability

CONTROL

Policy / authorization

EXECUTION

State / errors / retries

DEPENDENCY

External health / latency

EVIDENCE

Trace / artifact / receipt

RECOVERY RULE

Closure requires containment, causal explanation, restored service, reconciled intended vs observed state, preserved evidence, and an explicit residual-risk decision.

Deployment profiles and implementation roadmap

DEPLOYMENT PROFILES

PROFILE 01 **TRADITIONAL ROUTED CAMPUS MODERNIZATION**
Bounded proof

PROFILE 02 **LARGE EVPN/VXLAN CAMPUS FABRIC**
Team-scale governance

PROFILE 03 **CLOUD-MANAGED BRANCH AND WIRELESS ESTATE**
Sovereign / high-assurance

PROFILE 04 **HIGH-ASSURANCE SEGMENTED CAMPUS**
Distributed enterprise

IMPLEMENTATION ROADMAP



Progression is evidence-gated. Architecture adoption does not advance because a component is installed or demonstrated; each stage requires measurable service, safety, security, recovery, and evidence outcomes.

Verification plan, dependencies, and reading map

ACCEPTANCE CRITERIA - REPRESENTATIVE SET

AC-01	The architecture has a named service owner, technical owner, security owner, data owner, and recovery authority.	AC-02	The system boundary, external dependencies, retained responsibilities, and trust transitions are documented and
AC-03	Identity, authorization, secrets, policy, and privileged operations are explicit and independently auditable.	AC-04	Desired state, runtime state, observed state, and evidence state are distinguishable and reconciled.
AC-05	Consequential changes require preconditions, approval policy, bounded execution, verification, and rollback.	AC-06	Telemetry supports service health, security detection, forensic reconstruction, and conformance evidence.
AC-07	Failure modes include safe degradation, dependency loss, corrupted state, operator error, and malicious action.	AC-08	Backup, restoration, reconstitution, and exit procedures are exercised against defined recovery objectives.

RELATED REFERENCE ARCHITECTURES

No mandatory RA dependencies declared

MAPPED MYTHOS STANDARDS

MYTHOS-NET-0001, MYTHOS-NET-0005, MYTHOS-NET-0010, MYTHOS-NET-0011, MYTHOS-SEC-0007, MYTHOS-TEL-0001

DETAILED SPECIFICATION READING MAP

09	Executive direction	10	Scope and system context	12	Logical architecture
15	Flow contracts	16	Trust boundaries	17	Deployment profiles
20	Failure modes	21	Dependencies and standards	22	Implementation roadmap
23	Acceptance criteria	25	Metrics and decision gates	26	Source authority
27	Publication control				

The following pages preserve the detailed candidate architecture specification while this visual dossier adds explicit architecture diagrams, sequence views, state and evidence flows, observability, failure propagation, and implementation gates.

PART I - EXECUTIVE DIRECTION

OUTCOMES, RISKS, AND DECISIONS

ARCHITECTURE MANDATE

An identity-driven, observable, programmable campus, branch, wireless, WAN, and security architecture with explicit source of truth and change assurance.

EXECUTIVE OUTCOMES

- Deliver predictable user, device, application, and site connectivity.
- Bind access to identity, posture, role, and policy rather than physical location alone.
- Reduce failure domains through routed design, resilient services, and explicit local survivability.
- Operate the network from authoritative intent, telemetry, validation, and controlled change.

DECISIONS REQUIRED

- Accountable service and risk ownership.
- Accepted architecture profile and consequence class.
- Authoritative identity, data, policy, configuration, and evidence systems.
- Mandatory approval, recovery, privacy, safety, and supplier-exit gates.
- Funding for operations, observability, validation, and lifecycle—not only implementation.

PART II - SCOPE, PRINCIPLES, AND SYSTEM CONTEXT

NETWORK ENGINEERING

IN SCOPE

An identity-driven, observable, programmable campus, branch, wireless, WAN, and security architecture with explicit source of truth and change assurance.

OUT OF SCOPE

Vendor selection, exact sizing, contractual obligations, detailed low-level design, product certification, regulatory approval, and proof that any named platform is implemented.

ARCHITECTURE INVARIANTS

Explicit ownership; least authority; separable desired, runtime, observed, and evidence state; bounded automation; tested recovery; product-neutral interfaces; source and claim currency.

ASSUMPTIONS

Organizations tailor the pattern through documented risk, environment, criticality, data, safety, regulatory, workforce, and supplier analysis.

SYSTEM CONTEXT AND RESPONSIBILITY MODEL

ACTORS, ENVIRONMENTS, AND EXTERNAL DEPENDENCIES

ACTORS AND RESPONSIBILITY

- Service consumers and affected users
- Product, platform, network, security, data, reliability, and support teams
- Human administrators, operators, reviewers, incident commanders, and risk owners
- Machine identities, agents, workloads, devices, controllers, and external services
- Suppliers, providers, carriers, integrators, assessors, and regulators where applicable

RESPONSIBILITY BOUNDARY

- The adopting organization retains accountability for purpose, risk, configuration, data, identity, operation, recovery, and evidence even where a provider performs underlying functions.
- Inherited controls are recorded with provider, scope, evidence, limitations, shared responsibility, incident path, and exit conditions.
- No component is considered trusted solely because it is internal, managed, signed, cloud-hosted, model-generated, or supplied by a recognized vendor.

ARCHITECTURE POSITION

The architecture supports routed fabrics, wireless access, branch connectivity, segmentation, direct internet and cloud access, and policy enforcement without requiring a single vendor design.

PART III - LOGICAL ARCHITECTURE

LAYERS AND RESPONSIBILITIES

01**Physical and Underlay Fabric**

Physical and Underlay Fabric owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

02**Overlay and Segmentation**

Overlay and Segmentation owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

03**Identity and Access**

Identity and Access owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

04**Wireless and Edge Access**

Wireless and Edge Access owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

05**Branch, WAN, Internet, and Cloud**

Branch, WAN, Internet, and Cloud owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

06**Automation, Observability, and Assurance**

Automation, Observability, and Assurance owns a bounded set of responsibilities, interfaces, state, controls, failure behavior, telemetry, recovery procedures, and evidence. It does not silently absorb authority assigned to another layer.

CORE COMPONENTS - A

COMPONENTS 01-03

COMPONENT 01

Campus core, distribution, access, and spine-leaf fabric options

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

COMPONENT 02

VRF/VXLAN/EVPN or equivalent segmentation and routing

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

COMPONENT 03

802.1X, certificate, device profiling, guest, and privileged access policy

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

CORE COMPONENTS - B

COMPONENTS 04-06

COMPONENT 04

Wireless controllers or cloud control, access points, RF assurance, and client telemetry

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

COMPONENT 05

SD-WAN, internet, private WAN, SASE/ZTNA, DNS, DHCP, IPAM, and cloud connectivity

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

COMPONENT 06

Source of truth, configuration pipeline, streaming telemetry, synthetic tests, and change evidence

Required contract: owner, purpose, inputs, outputs, authority, data, dependencies, health, failure behavior, recovery, lifecycle, and evidence.

PART IV - DATA, CONTROL, AUTHORITY, AND EVIDENCE FLOW

FLOW CONTRACTS

1

Device and service intent is modeled before configuration.

Evidence: request and actor identity, policy decision, versions, state transitions, outputs, tests, errors, timing, and accountable disposition.

2

Identity and posture determine access and segment assignment.

Evidence: request and actor identity, policy decision, versions, state transitions, outputs, tests, errors, timing, and accountable disposition.

3

Traffic follows policy through local, WAN, internet, cloud, and security paths.

Evidence: request and actor identity, policy decision, versions, state transitions, outputs, tests, errors, timing, and accountable disposition.

4

Telemetry validates reachability, path, performance, experience, and policy.

Evidence: request and actor identity, policy decision, versions, state transitions, outputs, tests, errors, timing, and accountable disposition.

5

Change evidence reconciles intended, generated, deployed, and observed state.

Evidence: request and actor identity, policy decision, versions, state transitions, outputs, tests, errors, timing, and accountable disposition.

TRUST BOUNDARIES AND ENFORCEMENT

EVERY CROSSING REQUIRES AN EXPLICIT CONTRACT

TRUST BOUNDARY 01

Untrusted endpoint versus access edge

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

TRUST BOUNDARY 02

User/device identity versus authorization policy

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

TRUST BOUNDARY 03

Campus/branch segment versus shared services

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

TRUST BOUNDARY 04

Enterprise network versus internet, SaaS, and cloud

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

TRUST BOUNDARY 05

Management plane versus data plane

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

TRUST BOUNDARY 06

Vendor controller or cloud service versus local survivability

Minimum contract: authenticated parties, authorized actions, data classification, protocol, encryption, validation, rate and resource limits, observability, failure behavior, revocation, and evidence.

PART V - DEPLOYMENT PROFILES

PROFILE CHANGES SCALE, NOT ASSURANCE OUTCOMES

PROFILE 01 / TRADITIONAL ROUTED CAMPUS MODERNIZATION

Use this profile to establish a bounded implementation with explicit scale, criticality, users, data, autonomy, external dependencies, recovery objectives, staffing, and validation depth. The profile may simplify technology or topology but must preserve identity, least authority, evidence, safe failure, recovery, lifecycle, and accountable risk acceptance.

PROFILE 02 / LARGE EVPN/VXLAN CAMPUS FABRIC

Use this profile to establish a bounded implementation with explicit scale, criticality, users, data, autonomy, external dependencies, recovery objectives, staffing, and validation depth. The profile may simplify technology or topology but must preserve identity, least authority, evidence, safe failure, recovery, lifecycle, and accountable risk acceptance.

PROFILE 03 / CLOUD-MANAGED BRANCH AND WIRELESS ESTATE

Use this profile to establish a bounded implementation with explicit scale, criticality, users, data, autonomy, external dependencies, recovery objectives, staffing, and validation depth. The profile may simplify technology or topology but must preserve identity, least authority, evidence, safe failure, recovery, lifecycle, and accountable risk acceptance.

PROFILE 04 / HIGH-ASSURANCE SEGMENTED CAMPUS

Use this profile to establish a bounded implementation with explicit scale, criticality, users, data, autonomy, external dependencies, recovery objectives, staffing, and validation depth. The profile may simplify technology or topology but must preserve identity, least authority, evidence, safe failure, recovery, lifecycle, and accountable risk acceptance.

PART VI - OPERATING LIFECYCLE

FROM DISCOVERY THROUGH RETIREMENT



01 / Inventory and baseline

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

02 / Model addressing, topology, identity, and policy

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

03 / Validate design and failure domains

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

04 / Deploy in bounded site waves

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

05 / Verify user and application journeys

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

06 / Operate with telemetry and experience SLOs

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

07 / Reconcile drift and retire legacy paths

Entry and exit criteria, owner, evidence, exceptions, dependencies, rollback, and next decision are recorded. No phase is complete solely because components were purchased, configured, or demonstrated.

SECURITY, PRIVACY, SAFETY, AND RIGHTS

CROSS-CUTTING ASSURANCE

SECURITY

Threat model identities, trust boundaries, supply chain, control planes, data, protocols, privilege, abuse, detection, response, recovery, and residual risk.

PRIVACY

Purpose limitation, minimization, transparency, consent where required, access, correction, retention, deletion, sovereignty, metadata, and third-party processing.

SAFETY

Hazards, unsafe states, human intervention, physical consequence, dependency failure, automation limits, emergency stop, recovery sequence, and validation.

RIGHTS AND USABILITY

Accessibility, contestability, explanation, operator workload, affected-user communication, grievance, misuse prevention, and equitable performance.

SUPPLY CHAIN

Provenance, version, SBOM or component inventory, signature, vulnerability, support, update, provider, subcontractor, and exit.

EVIDENCE

Design decisions, tests, telemetry, incidents, approvals, exceptions, recovery exercises, source currency, and review findings remain linked to the architecture version.

FAILURE MODES AND RESILIENCE

DESIGN FOR SAFE DEGRADATION AND TRUSTWORTHY RECOVERY

FAILURE SCENARIO 01

Identity service failure blocks access or falls back too broadly.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

FAILURE SCENARIO 02

Layer 2 scope or control-plane convergence creates a campus-wide failure.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

FAILURE SCENARIO 03

Wireless interference, channel design, or client behavior defeats nominal coverage.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

FAILURE SCENARIO 04

SD-WAN policy sends traffic through an unsafe or congested path.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

FAILURE SCENARIO 05

DNS, DHCP, IPAM, certificate, time, or cloud-control dependencies fail.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

FAILURE SCENARIO 06

Generated configuration differs from device behavior or operational state.

Required response: detect, contain, preserve evidence, maintain or enter safe service, communicate, recover, verify, learn, and prevent recurrence.

PART VII - INTEGRATION AND DEPENDENCY MODEL

CONNECTED REFERENCE ARCHITECTURES AND STANDARDS

REFERENCE ARCHITECTURE DEPENDENCIES

- RA-004 - Network Source of Truth Implementation Pipeline
- RA-009 - Zero-Trust Identity, Policy, Secrets, and Access Fabric
- RA-011 - Digital Twin, Infrastructure Automation, and Change Assurance
- RA-012 - Enterprise Observability, SRE, and Incident Command Platform
- RA-015 - Edge, OT, IoT, and Telecommunications Convergence

MAPPED MYTHOS STANDARDS

- MYTHOS-NET-0001
- MYTHOS-NET-0005
- MYTHOS-NET-0010
- MYTHOS-NET-0011
- MYTHOS-SEC-0007
- MYTHOS-TEL-0001

DEPENDENCY DOCTRINE

A dependency is not a blanket trust grant. Each connection requires an interface, identity, policy, data, availability, version, failure, recovery, and evidence contract. Correlated failure and circular authority must be analyzed across the full architecture graph.

PART VIII - IMPLEMENTATION AND ADOPTION ROADMAP

PHASED, EVIDENCE-DRIVEN TRANSITION

0-30 DAYS

Inventory purpose, owners, users, systems, data, dependencies, risks, current diagrams, incidents, recovery, and evidence gaps.

31-90 DAYS

Establish authoritative identity, configuration, policy, data, source, and architecture records; define target profile and acceptance tests.

3-6 MONTHS

Implement bounded foundations, isolation, telemetry, change control, backup, recovery, and representative pilot workflows.

6-12 MONTHS

Expand through standard patterns, automation, service ownership, SLOs, independent assessment, failure injection, and supplier-exit exercises.

ONGOING

Reconcile drift, review sources, reassess risk, measure outcomes, exercise recovery, renew exceptions, migrate dependencies, and retire obsolete paths.

ARCHITECTURE ACCEPTANCE CRITERIA - A

CRITERIA 01-09

AC-01

The architecture has a named service owner, technical owner, security owner, data owner, and recovery authority.

AC-02

The system boundary, external dependencies, retained responsibilities, and trust transitions are documented and reviewed.

AC-03

Identity, authorization, secrets, policy, and privileged operations are explicit and independently auditable.

AC-04

Desired state, runtime state, observed state, and evidence state are distinguishable and reconciled.

AC-05

Consequential changes require preconditions, approval policy, bounded execution, verification, and rollback.

AC-06

Telemetry supports service health, security detection, forensic reconstruction, and conformance evidence.

AC-07

Failure modes include safe degradation, dependency loss, corrupted state, operator error, and malicious action.

AC-08

Backup, restoration, reconstitution, and exit procedures are exercised against defined recovery objectives.

AC-09

Data classification, retention, privacy, sovereignty, and disposition controls follow the actual information flow.

ARCHITECTURE ACCEPTANCE CRITERIA - B

CRITERIA 10-18

AC-10

Supplier, model, protocol, platform, and software dependencies have provenance, version, support, and replacement records.

AC-11

Representative performance and capacity tests include saturation, contention, latency, and degraded conditions.

AC-12

Exceptions are time-bounded, visible, approved by accountable risk owners, and linked to compensating controls.

AC-13

Every site has documented underlay, overlay, identity, service, management, security, and failure-domain diagrams.

AC-14

Access policy is tested for employees, administrators, contractors, guests, unmanaged devices, IoT, voice, and emergency operations.

AC-15

DNS, DHCP, IPAM, certificate, time, identity, telemetry, and management dependencies have local or tested degraded modes.

AC-16

Wireless assurance includes spectrum, channel, power, capacity, roaming, client compatibility, and application-experience evidence.

AC-17

WAN path policy is validated under carrier loss, brownout, asymmetric routing, SaaS failure, and security-service failure.

AC-18

A representative site can be rebuilt from authoritative data, signed artifacts, and documented bootstrap dependencies.

METRICS, EVIDENCE, AND DECISION GATES

MEASURE SERVICE OUTCOMES AND ASSURANCE

COVERAGE

Percent of components, interfaces, identities, data flows, dependencies, risks, and controls represented in current architecture evidence.

CHANGE QUALITY

Plan success, rollback, verification pass, escaped defect, drift, and emergency-change rates.

RELIABILITY

Availability, latency, saturation, dependency health, recovery time, recovery point, and safe-degradation success.

SECURITY

Privilege exposure, policy denial, identity compromise, vulnerable dependency, detection coverage, response, and evidence completeness.

HUMAN OUTCOME

Task success, operator workload, accessibility, override, contestability, training, and user-impact measures.

LIFECYCLE

Version currency, unsupported component, exception age, migration readiness, restore exercise, and retirement completeness.

Release or expansion gate: mandatory acceptance criteria pass; failed safety, privacy, identity, recovery, evidence, or legal gates block promotion regardless of aggregate score.

SOURCE AUTHORITY REGISTER

CURRENT PRIMARY AND OFFICIAL REFERENCES

SOURCE 01 NIST SP 800-207, Zero Trust Architecture

<https://csrc.nist.gov/pubs/sp/800/207/final>

SOURCE 02 NIST SP 1800-35, Implementing a Zero Trust Architecture

<https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture>

SOURCE 03 RFC 8345, YANG Data Model for Network Topologies

<https://www.rfc-editor.org/info/rfc8345>

SOURCE 04 RFC 8969, Framework for Automating Service and Network Management

<https://www.rfc-editor.org/info/rfc8969>

SOURCE 05 OpenConfig Vendor-Neutral Network Models

<https://www.openconfig.net/>

SOURCE 06 OpenTelemetry Specification

<https://opentelemetry.io/docs/specs/>

Source currency note. Official frameworks, specifications, and implementation guidance evolve. Assessors must verify the current version, status, errata, applicability, and effective date at adoption and scheduled review. NIST AI RMF 1.0 was under revision at the publication date.

PUBLICATION CONTROL AND REVISION

PERMANENT IDENTITY / CONTROLLED EVOLUTION

PERMANENT DOCUMENT IDENTITY	RA-003
VERSION	1.0.0-candidate
PUBLICATION DATE	2026-07-24
SCHEDULED REVIEW	2027-01-24
STATUS	Candidate Reference Architecture
ARCHITECTURE SET	Canonical Set
CLASSIFICATION	Public
PUBLISHER	Mythos Systems

REVISION RECORD

1.0.0-candidate (2026-07-24) - Permanent-publication candidate edition regenerated under the Mythos Systems architecture publication system. Production sequence metadata is excluded from public identity.