

SYS-47

NET-93

AI-02

AI-DRIVEN NETWORK AUTOMATION

BEST PRACTICES FOR BUILDING TOOLS WITH AGENTS

SYS-47

NETWORK ARCHITECT & AUTOMATION ADVOCATE

NET-93

SPENDING YEARS IN THE TRENCHES MANAGING COMPLEX INFRASTRUCTURE, I FOCUS ON MOVING FROM MANUAL CLI CONFIGURATIONS TO INFRASTRUCTURE AS CODE (IAC).

AI-02

- SOURCE OF TRUTH (SOT) EVANGELIST.
- EXPLORING THE BLEEDING EDGE OF AI IN NETOPS.
- GOAL: MAKING THE NETWORK DECLARATIVE, AUTONOMOUS, AND FUN AGAIN.



SYS-47

NET-93

AI-02

DATABASE: THE AI PRIMER

LEARNING THE MECHANICS OF AI CODING ARCHITECTURES.

SYS-47

LARGE LANGUAGE MODELS (THE ENGINE)

NET-93

AN LLM IS FUNDAMENTALLY A MASSIVE PATTERN RECOGNITION AND PREDICTION ENGINE. IT DOESN'T "THINK," IT CALCULATES THE STATISTICALLY MOST LIKELY NEXT WORD BASED ON ITS TRAINING DATA.

AI-02

FOR CODING, IT ACTS AS AN AUTOCOMPLETE ON STERIODS, UNDERSTANDING SYNTAX ACROSS PYTHON, YAML, AND JINJA NATIVELY.

SYSTEM PROMPTS (THE STEERING WHEEL)

IF THE LLM IS THE ENGINE, THE PROMPT IS THE STEERING WHEEL. A SYSTEM PROMPT DEFINES THE AI'S PERSONA, ITS RULES, AND ITS BOUNDARIES.

INSTEAD OF "WRITE A SCRIPT," WE SAY: "YOU ARE AN EXPERT NETWORK ENGINEER. WRITE IDEMPOTENT PYTHON UTILIZING THE SOURCE OF TRUTH REST API..."

SYS-47

AN LLM ALONE IS JUST A BRAIN IN A JAR. AN **AGENT** IS A BRAIN WITH HANDS.

NET-93

- **AUTONOMY:** AGENTS USE A LOOP (LIKE REACT: REASON + ACT) TO BREAK DOWN COMPLEX TASKS INTO SMALLER STEPS.

AI-02

- **MEMORY:** THEY KEEP A CONTEXT WINDOW OF WHAT THEY HAVE TRIED, WHAT WORKED, AND WHAT FAILED.
- **EXECUTION:** UNLIKE STANDARD CHAT INTERFACES WHERE YOU COPY/PASTE, AN AGENT CAN EXECUTE CODE ON YOUR BEHALF AND READ THE OUTPUT.



SYS-47

NET-93

AI-02



TOOLS (PRIMITIVES)

TOOLS ARE THE BASIC FUNCTIONS EXPOSED TO THE AI. "READ_FILE", "WRITE_FILE", "EXECUTE_CMD". THEY ARE THE RAW ACTIONS THE AGENT CAN TAKE ON A SYSTEM.



SKILLS (COMPLEX)

SKILLS ARE HIGHER-LEVEL CAPABILITIES BUILT FROM TOOLS. INSTEAD OF JUST BASH, A SKILL MIGHT BE "DEPLOY_PLUGIN" OR "RUN_BGP_TEST".



EXECUTION

WHEN GIVEN A GOAL, THE AGENT SEARCHES ITS INVENTORY OF TOOLS AND SKILLS TO FIGURE OUT HOW TO INTERACT WITH THE ENVIRONMENT TO ACHIEVE THE OBJECTIVE.

SYS-47

NET-93

AI-02



THE UNIVERSAL PLUG (MCP)

HISTORICALLY, GIVING AN AI TOOLS MEANT WRITING CUSTOM, BRITTLE API INTEGRATIONS FOR EVERY SINGLE LLM PROVIDER.

MCP IS THE UNIVERSAL STANDARD OF AI. IT ALLOWS YOU TO DEFINE DATA SOURCES AND TOOLS ONCE, AND SECURELY EXPOSE THEM TO ANY COMPATIBLE AI AGENT. WE USE MCP TO SECURELY HOOK THE AGENT INTO OUR NETWORK SOURCE OF TRUTH.

SYS-47

NET-93

AI-02

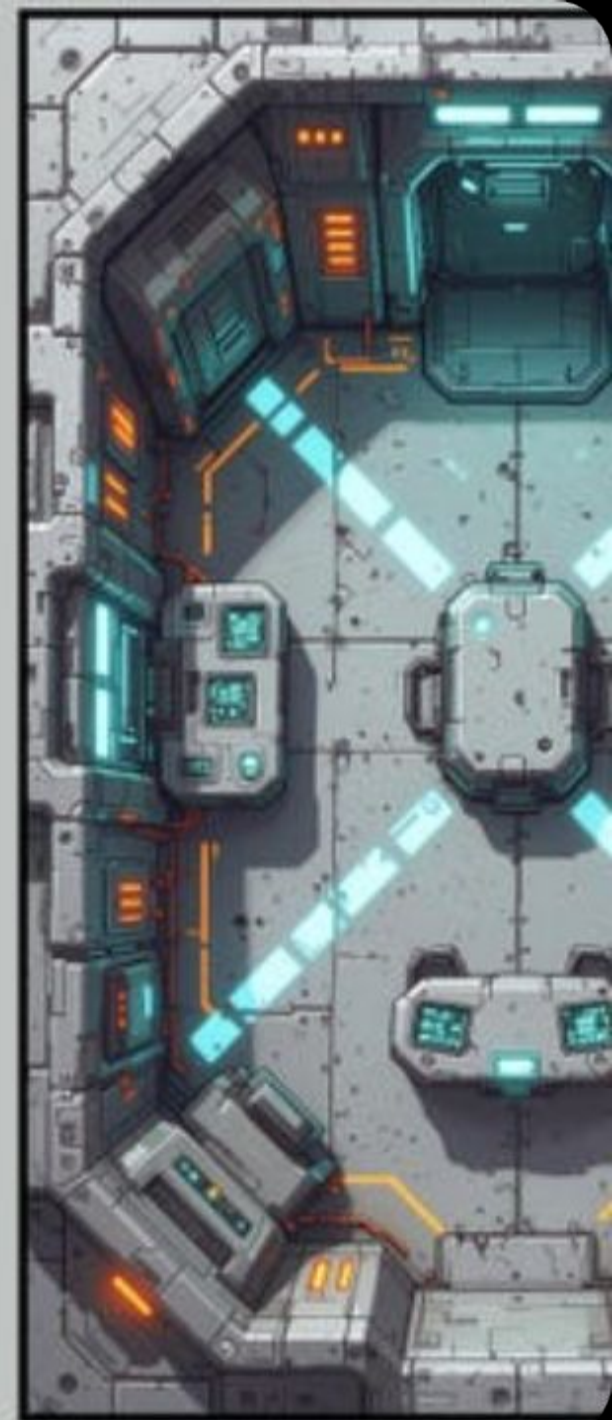
MISSION: THE DIGITAL TWIN

BUILDING A SOURCE OF TRUTH PLUGIN ALONGSIDE AN AI AGENT.

PRIMARY OBJECTIVE

OPEN-SOURCE DIGITAL TWIN

WE WANTED TO BUILD A NETWORK DIGITAL TWIN PLUGIN LIVING DIRECTLY INSIDE OUR SOURCE OF TRUTH, ALLOWING US TO MODEL STATE AND VERIFY OPERATIONAL INTENT.



DEVICE SCOPE

Name * Lab Devices Live Scope

Description Live collection scope for lab devices

Scope type * Static

Dynamic group -----

Devices ABR × CE1 × CE2 × EIGRP1 × NX1 × NX2 × P × PE1 × PE2 × RIP1 × SW1 × ×
SW2 ×

Virtual machines -----

Secrets group -----

Fallback secrets group for members without their own (e.g. virtual machines).

SYS-47

NET-93

AI-02



SYS-47

NET-93

AI-02

REACHABILITY QUERY

Snapshot

Lab Devices Live Scope @ Apr 13, 2026, 8:56 AM CDT

Source IPAM Address

10.10.20.10/24

Select a Nautobot IPAM address as the source, or enter manually below.

Destination IPAM Prefix

Select a Nautobot IPAM prefix. All host addresses in the prefix will be expanded as destinations.

Destination IPs (manual)

[Empty text input field for manual destination IPs]

Comma-separated explicit destination IPs (max 16). Used when no IPAM selection is made above.

Protocol

TCP

Port

80

Max paths

8

Maximum number of equal-cost paths to return.

Max hops

16

Maximum hop count before path tracing stops.

Max recursion depth

8

Maximum recursive next-hop resolution depth.

Enforce security policy checks

Run Query

Source IP (manual)

[Empty text input field for manual source IP]

Manual source IP. Ignored when an IPAM address is selected above.

Destination IPAM Addresses

1.1.1.1/32

Select Nautobot IPAM addresses as destinations.



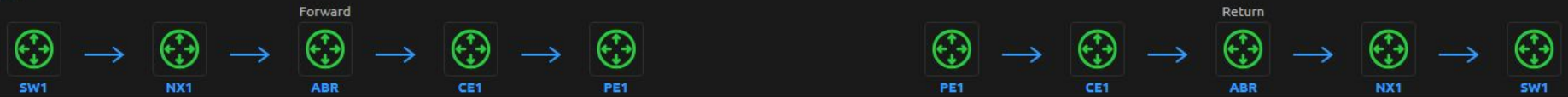
SYS-47

NET-93

AI-02

PATH DIAGRAM

1.1.1.1 REACHABLE



RESULTS

Destination	Verdict	Confidence	Root Cause	Security	Forward	Reverse	Summary	Forward Paths	Reverse Paths
1.1.1.1	REACHABLE	HIGH	END_TO_END_REACHABLE	PASS	PASS	PASS	Reachability computed from snapshot state.	1 1. SW1 STATIC VRF LAB Prefix 0.0.0.0/0 In Vlan20 Out Gi0/1 2. NX1 OSPF-10 VRF default Prefix 1.1.1.1/32 In Vlan20 Out Eth1/1 3. ABR OSPF VRF default Prefix 1.1.1.1/32 In GigabitEthernet0/3 Out GigabitEthernet0/1 4. CE1 BGP VRF default Prefix 1.1.1.1/32 In GigabitEthernet0/2 Out GigabitEthernet0/1 5. PE1 N/A VRF default Prefix In GigabitEthernet3 Out Loopback0	1 CONNECTED 1. PE1 BGP VRF default Prefix 10.10.20.0/24 In Loopback0 Out GigabitEthernet3 2. CE1 OSPF VRF default Prefix 10.10.20.0/24 In GigabitEthernet0/1 Out GigabitEthernet0/2 3. ABR OSPF VRF default Prefix 10.10.20.0/24 In GigabitEthernet0/1 Out GigabitEthernet0/3 4. NX1 DIRECT VRF default Prefix 10.10.20.0/24 In Eth1/1 Out Eth1/3 5. SW1 N/A VRF LAB Prefix In ? Out Vlan20

REACHABILITY QUERY

Snapshot

Lab Devices Live Scope @ Apr 13, 2026, 9:02 AM CDT

Source IPAM Address

10.10.20.10/24

Select a Nautobot IPAM address as the source, or enter manually below.

Destination IPAM Prefix

Select a Nautobot IPAM prefix. All host addresses in the prefix will be expanded as destinations.

Destination IPs (manual)

Comma-separated explicit destination IPs (max 16). Used when no IPAM selection is made above.

Protocol

TCP

Port

80

Max paths

8

Maximum number of equal-cost paths to return.

Max hops

16

Maximum hop count before path tracing stops.

Max recursion depth

8

Maximum recursive next-hop resolution depth.

Enforce security policy checks

Run Query

Source IP (manual)

Manual source IP. Ignored when an IPAM address is selected above.

Destination IPAM Addresses

1.1.1.1/32

Select Nautobot IPAM addresses as destinations.

SYS-47

NET-93

AI-02

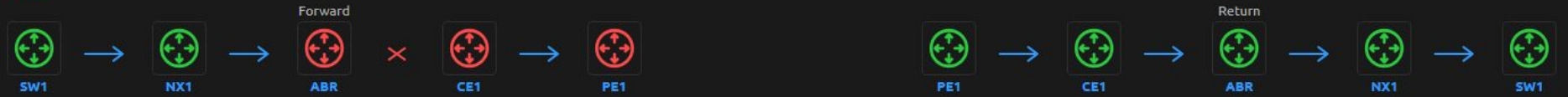
SYS-47

NET-93

AI-02

PATH DIAGRAM

1.1.1.1 UNREACHABLE



RESULTS

Destination	Verdict	Confidence	Root Cause	Security	Forward	Reverse	Summary	Forward Paths	Reverse Paths
1.1.1.1	UNREACHABLE	HIGH	SECURITY_POLICY_DENY	FAIL	PASS	PASS	Security policy denied the flow.	1 SW1 STATIC VRF LAB Prefix 0.0.0.0/0 In Vlan20 Out Gi0/1 2. NX1 OSPF-10 VRF default Prefix 1.1.1.1/32 In Vlan20 Out Eth1/1 3. ABR OSPF VRF default Prefix 1.1.1.1/32 In GigabitEthernet0/3 Out GigabitEthernet0/1 4. CE1 BGP VRF default Prefix 1.1.1.1/32 In GigabitEthernet0/2 Out GigabitEthernet0/1 5. PE1 N/A VRF default Prefix In GigabitEthernet3 Out Loopback0	1 PE1 BGP VRF default Prefix 10.10.20.0/24 In Loopback0 Out GigabitEthernet3 2. CE1 OSPF VRF default Prefix 10.10.20.0/24 In GigabitEthernet0/1 Out GigabitEthernet0/2 3. ABR OSPF VRF default Prefix 10.10.20.0/24 In GigabitEthernet0/1 Out GigabitEthernet0/3 4. NX1 DIRECT VRF default Prefix 10.10.20.0/24 In Eth1/1 Out Eth1/3 5. SW1 N/A VRF LAB Prefix In ? Out Vlan20



SYS-47

NET-93

AI-02



SNAPSHOT DIFF

Device scope

Lab Devices Live Scope

Newer snapshot

Lab Devices Live Scope @ Apr 13, 2026, 9:02 AM CDT



Older snapshot

Lab Devices Live Scope @ Apr 13, 2026, 8:56 AM CDT

Diff runs automatically once both snapshots are selected.

SUMMARY

Newer Snapshot Totals

Newer-only rows: **2**

Older-only rows: **0**

Modified rows: **0**

Total changes on newer side: **2**

Older Snapshot Totals

Newer-only rows: **2**

Older-only rows: **0**

Modified rows: **0**

Total changes on older side: **0**

CHANGES

Added 1 Device

- ABR

ACL Rule

Newer snapshot (newer-only): Lab Devices Live Scope @ April 13, 2026, 2:02 p.m. UTC

Older snapshot: Lab Devices Live Scope @ April 13, 2026, 1:56 p.m. UTC

```
acl_name: DENY_80
action: DENY
dst_prefix: ''
order: 10
port: 80
protocol: '6'
src_prefix: ''
virtual_machine: null
```

No matching row in older snapshot.

```
acl_name: DENY_80
action: ALLOW
dst_prefix: ''
order: 20
port: null
protocol: ''
src_prefix: ''
virtual_machine: null
```

No matching row in older snapshot.

SYS-47

NET-93

AI-02

**AI AGENTS ARE INCREDIBLY FAST CODERS, BUT
THEY ARE TERRIBLE MIND READERS. IF IT'S NOT IN
THE SPEC, IT WON'T BE IN THE CODE.**

*PROTOCOL: USE A CONVERSATIONAL AI STRICTLY FOR BRAINSTORMING TO GENERATE A
HYPER-DETAILED ARCHITECTURAL SPECIFICATION DOCUMENT BEFORE THE CODING
AGENT STARTS.*

SYS-47

NET-93

AI-02



THE SPECIFIER

RESPONSIBLE FOR ANALYZING THE PROJECT GOAL AND GENERATING A COMPREHENSIVE, MACHINE-READABLE SPECIFICATION DOCUMENT THAT OUTLINES EXACTLY WHAT NEEDS TO BE BUILT.



THE IMPLEMENTER

READS THE SPECIFICATION DOCUMENT AND STRICTLY EXECUTES THE CODE GENERATION. THIS PERSONA FOCUSES ENTIRELY ON SYNTAX AND ADHERING TO THE DEFINED ARCHITECTURE.



THE VALIDATOR

EVALUATES THE GENERATED CODEBASE AGAINST THE ORIGINAL SPECIFICATION. RUNS TESTS, CHECKS STATE, AND FEEDS ANY REQUIRED CORRECTIONS BACK TO THE IMPLEMENTER.

SYS-47

NET-93

AI-02

03

DEBUGGING AUTONOMY

GIVING THE AGENT EYES

WE GAVE THE CODING AGENT THE ABILITY TO EXECUTE UNIT TESTS AND PYTHON LINTING ON ITS OWN CODE AS IT WAS BEING WRITTEN.

BY EXPOSING TERMINAL ACCESS WITHIN A SANDBOX, THE AGENT COULD READ THE PYTHON TRACEBACKS, IDENTIFY ITS OWN SYNTAX ERRORS, AND FIX SOURCE OF TRUTH PLUGIN CRASHES BEFORE HUMAN REVIEW.

SYS-47

NET-93

AI-02

DEV SERVER DEPLOYMENT

A DIGITAL TWIN IS USELESS IF IT ONLY WORKS IN A TEXT FILE. WE CREATED A SPECIFIC "SKILL" FOR THE AGENT TO AUTONOMOUSLY DEPLOY ITS DRAFTED PLUGIN CODE VIA DOCKER TO A LOCAL DEVELOPMENT SOURCE OF TRUTH SERVER.

MOCK LAB EXECUTION

ONCE DEPLOYED, THE AGENT WAS GRANTED ANOTHER SKILL TO TRIGGER AUTOMATION JOBS THAT RAN SIMULATIONS AGAINST A MOCKED LAB NETWORK TO VERIFY ITS ROUTING LOGIC AND OVERALL VALIDITY.

SYS-47



KNOWN GOOD SCENARIOS: WE PROVIDED THE AGENT WITH PRE-VALIDATED NETWORK TOPOLOGIES AND EXPECTED ROUTING OUTCOMES TO USE AS ITS BASELINE TESTING STANDARD.

NET-93



LAB DEVICE ACCESS: WE GAVE THE AGENT READ-ONLY SSH ACCESS VIA A PROXY TOOL TO SAFELY LOGIN TO ACTUAL LAB ROUTERS TO GATHER REAL-TIME STATE.

AI-02



STATE COMPARISON: THE AGENT AUTONOMOUSLY GATHERED ACTUAL ROUTING TABLE OUTPUTS AND COMPUTATIONALLY COMPARED THEM AGAINST THE RESULTS ITS DIGITAL TWIN CODE WAS PREDICTING.

SYS-47

NET-93

AI-02



FOR THE USERS

WE INSTRUCTED THE AI TO AUTOMATICALLY GENERATE THE USER-FACING DOCUMENTATION, INCLUDING SETUP INSTRUCTIONS, FEATURE WALK-THROUGHS, AND UI NAVIGATION GUIDES BASED ON THE CODE IT JUST WROTE.



FOR THE DEVELOPERS

THE AI HANDLED THE GENERATION OF COMPREHENSIVE DEVELOPER DOCUMENTATION: POPULATING CODE COMMENTS, GENERATING ARCHITECTURAL DIAGRAMS, AND MAPPING OUT THE API REFERENCES.



FOR FUTURE AGENTS

CRUCIALLY, THE AI WROTE MACHINE-READABLE DOCUMENTATION. THIS ESSENTIALLY PACKAGES THE NEW PROJECT FEATURES INTO NEW "SKILLS" FOR FUTURE AI AGENTS TO IMMEDIATELY UTILIZE AND EXPAND UPON.

SYS-47

IF I WERE TO DEVELOP THIS, WHAT WOULD I NEED?

NET-93

- A VISION OF SOMETHING TO BUILD
- EXPECTATIONS & REQUIREMENTS

- TEST ENVIRONMENT TO ITERATE AGAINST
- SECURITY GUIDELINES OR RESTRICTIONS

AI-02

- GUIDELINES & RESTRICTIONS
- ARCHITECTURE & PRE-REQUISITES

- DOCUMENTATION, AUDIENCE, UI/UX EXPECTATIONS
- EXPANDABLE, FUTURE PLANS, ROADMAPS

END OF PROGRAM

COMMUNICATION CHANNEL OPEN FOR INQUIRIES.

> WAITING FOR INPUT...

SYS-47

NET-93

AI-02