
codilime
From Chaos to Clarity
AI-Driven Network Troubleshooting

Tomasz Janaszka, PhD

Solutions architect

Adam Kułagowski

Principal network engineer

Monika Antoniak

Director of Engineering & Professional Services

Agenda

- Solution architecture
- Network topology and configuration
- Net-Inspector app
- Exercises
- MCP and AI-agentic apps
- Workshop summary

Disclaimer

Today you will play with the Net-Inspector (an application built just for AutoCon4), a GenAI-based solution for network troubleshooting.

Please keep in mind that this tool:

- may hallucinate and produce inaccurate results
- may get stuck might run out of context window of used LLM
- might call other tools than expected by network engineer

This is left unadjusted intentionally to show the potential dangers and limitations associated with using these types of tools

Challenges

- Autocon 2 (Net-Chat Assistant)
  - Small network topology
  - Simple network setup
  - LangChain ReAct Agent
  - LLM (gpt-4o-mini) 120k CW
- Autocon 4 (Net-Inspector)
  - Large network topology
  - Complex network setup
  - Complex networking data
  - MCP protocol/server/client
  - Better and more powerful LLMs, agentic frameworks

- **How to build valuable and supporting AI-agents working with networking data**
- **Where are we concerning maturity of LLMs, Agentic Frameworks, MCP**

Objectives of the workshop

- Explore and understand a large network topology through a hands-on interface.
- Interact with a chat interface backed by a multi-tool AI ReAct agent (network topology, control-plane, data-plane, syslog & alert tools).
- Identify misconfigurations and troubleshoot real-world issues using the Net-Inspector application, assessing agent readiness at scale.
- Learn the MCP protocol and its role in orchestrating tools and AI agents.
- Assess the practical effort, limitations and maturity of LLM-supported AI-agent technology in large-scale network problems.
- See how changing LLM models impacts the quality of results

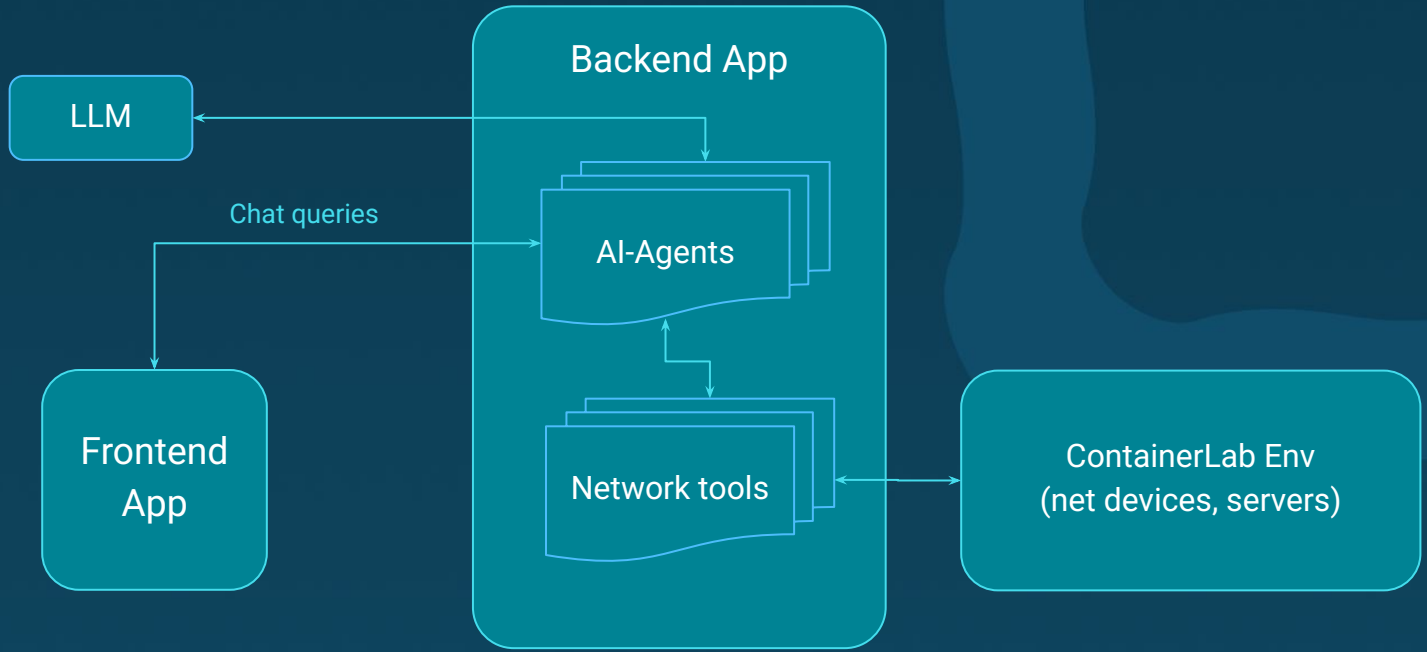
Net-Inspector

Introduction to Net-Inspector

- Architecture
- MCP servers
- AI-agents + MCP tools

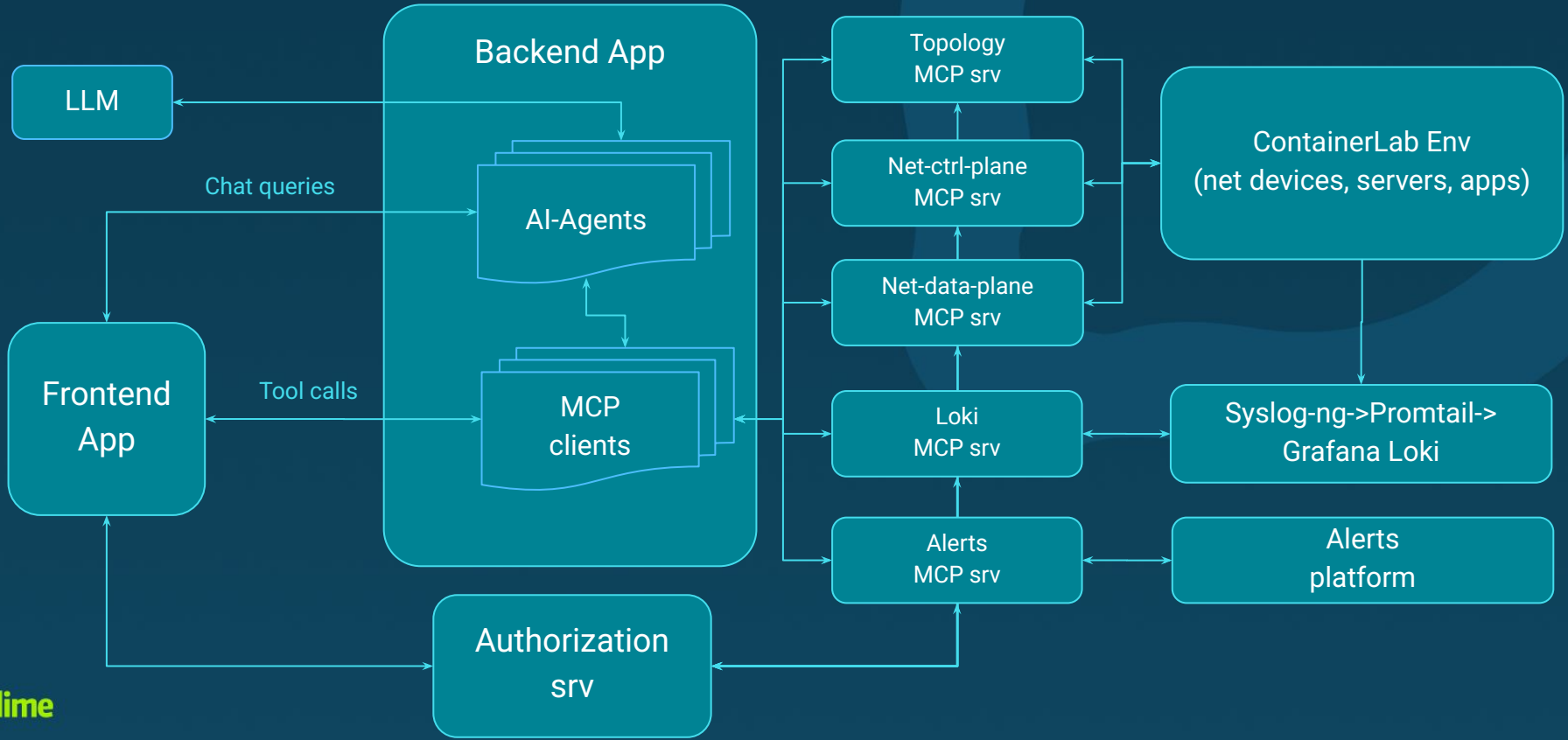
Architecture

Introduction to Net-Chat Assistant (Autocon 2)



Architecture

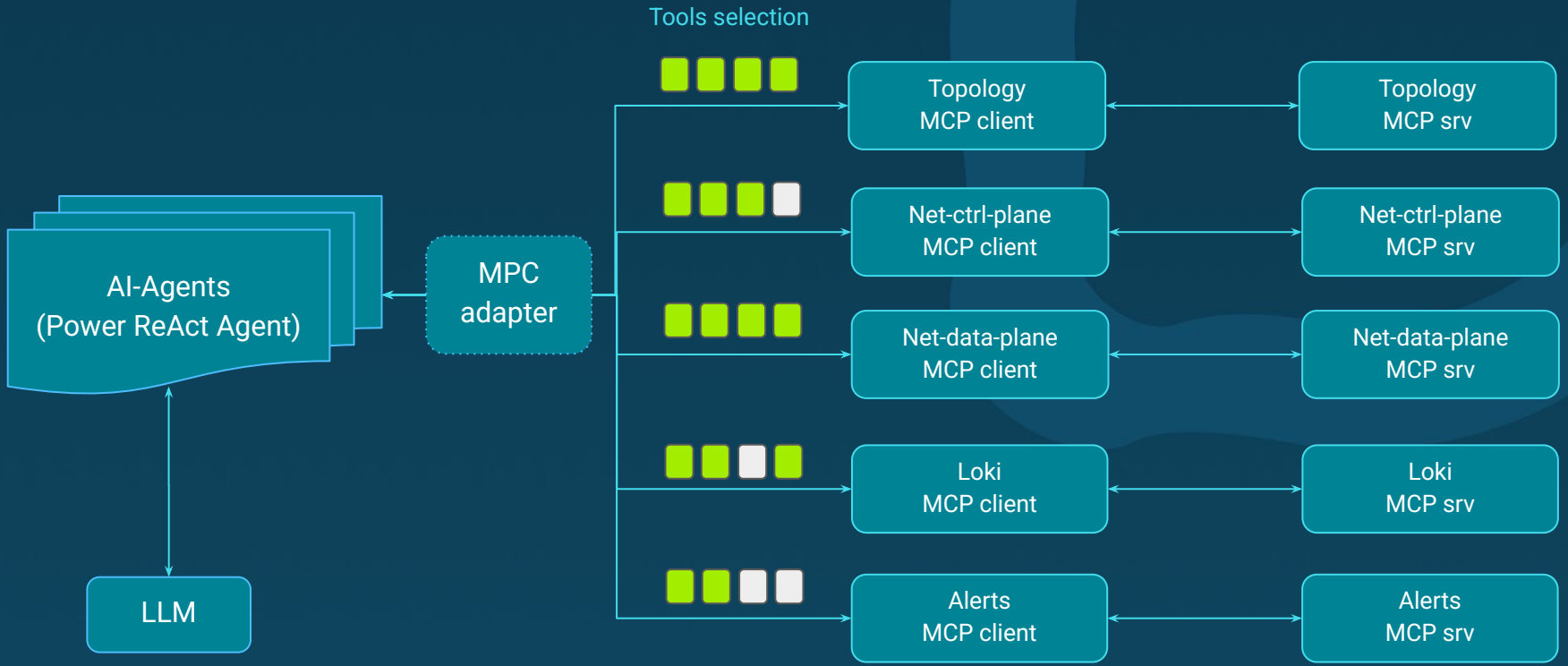
Introduction to Net-Inspector



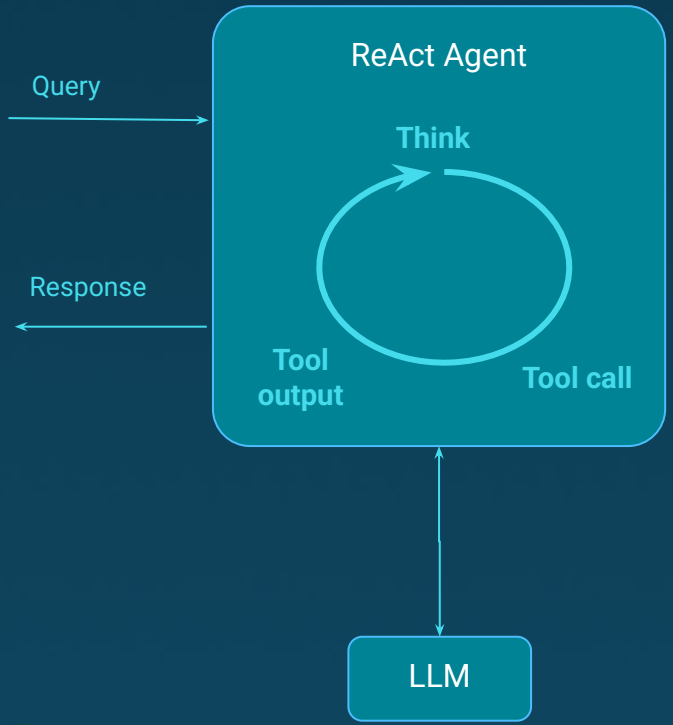
Introduction to Net-Inspector

Topology MCP srv	Tools related to topology data on nodes and links
Net-ctrl-plane MCP srv	Tools related to network control plane (executed on nodes)
Net-data-plane MCP srv	Tools related to network data plane (executed on nodes)
Loki MCP srv	Tools related to retrieval of syslog data (executed on loki server)
Alerts MCP srv	Tools related to retrieval of alerts (simple functionality prepared for workshop)

Introduction to Net-Inspector

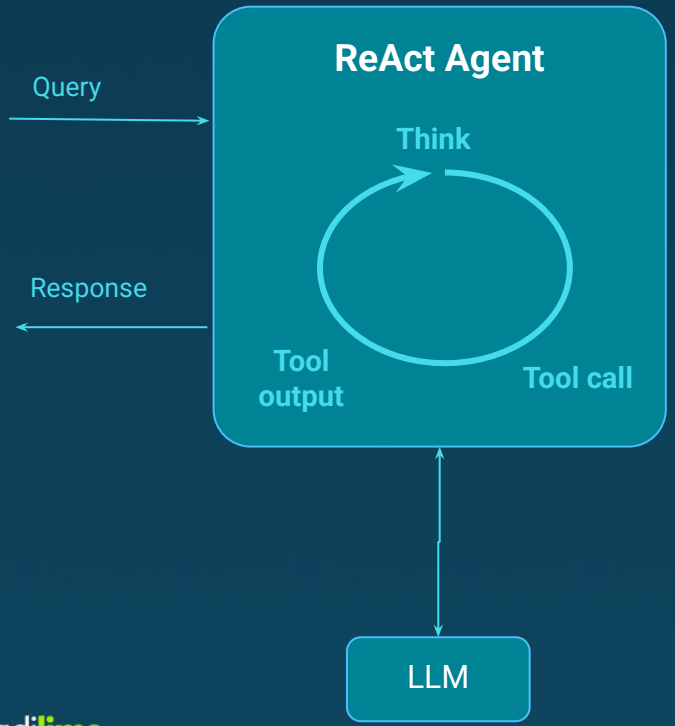


Introduction to Net-Inspector



- Think: Query + Available tools + Tool output
- Select and parametrize particular tool
- Interpret tool output
- Decide on stop or next step
- Format response

Introduction to Net-Inspector



- General queries and not precise initial context are challenging
- Many tools not precisely described mislead LLM/ReAct
- Complex and rich network data is challenging
- LLM reasoning capabilities are crucial
- Large LLM context window size, but higher hallucinations
- Sequential loop think/act/interpret means long response time

Topology

Introduction to network setup

- Challenges
- Devices
- Services
- Miscellaneous

Challenges

- Emulating large topology
  - Memory & CPU constraints of VM
- Rich Controle Plane features
  - Data plane must keep up
- Realistic network
  - Topology
  - Devices and services
- Fully automatic generation & deployment

Challenges - scale

Latest member of virtual lab family:

- emphasis on containers
- entire lab in a single YAML
- device images downloaded automatically
- device provisioning

Version 0.71.1 is used

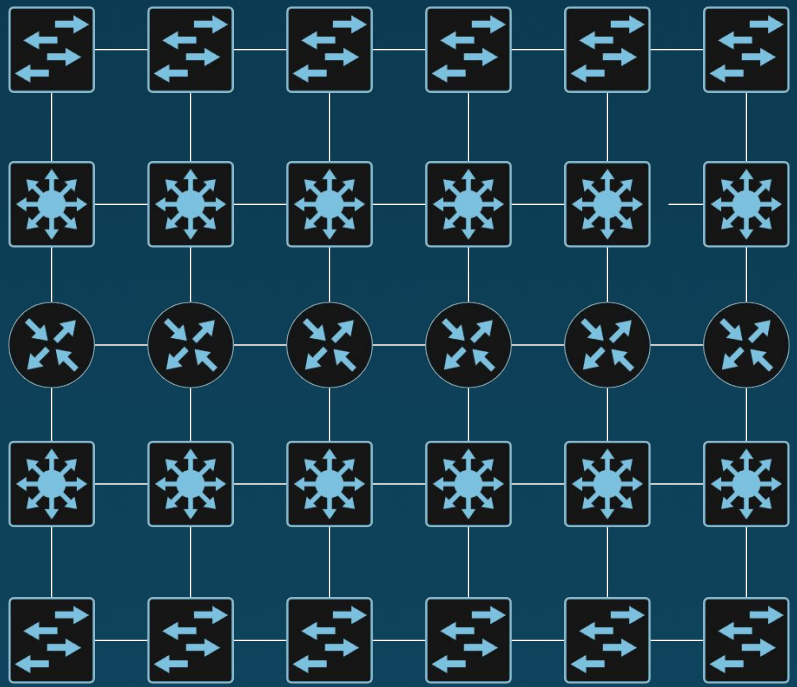
Challenges - CP & DP

FRRouting

- is an IP routing suite
- can be run in container
- supports BGP, BFD, IS-IS, LDP, MPLS
  - and others
- Cisco-like CLI
- can utilize Linux kernel as Data Plane

Version 15.0 is being used

Challenges - topology



Things to avoid

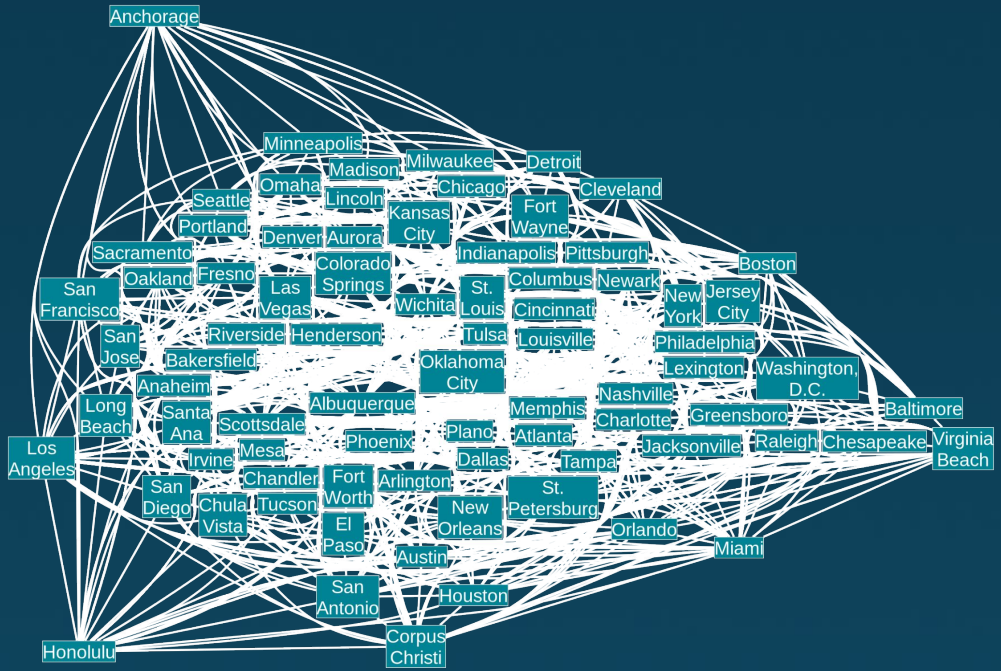
- Artificial looking topologies:
  - Ring / Matrix
- Lack of redundancy
- Topologies with limited no. of protocols
  - Spine & Leaf

Challenges - topology

ISP topology

- Based on maps & cities
- Has all protocols
- Complex

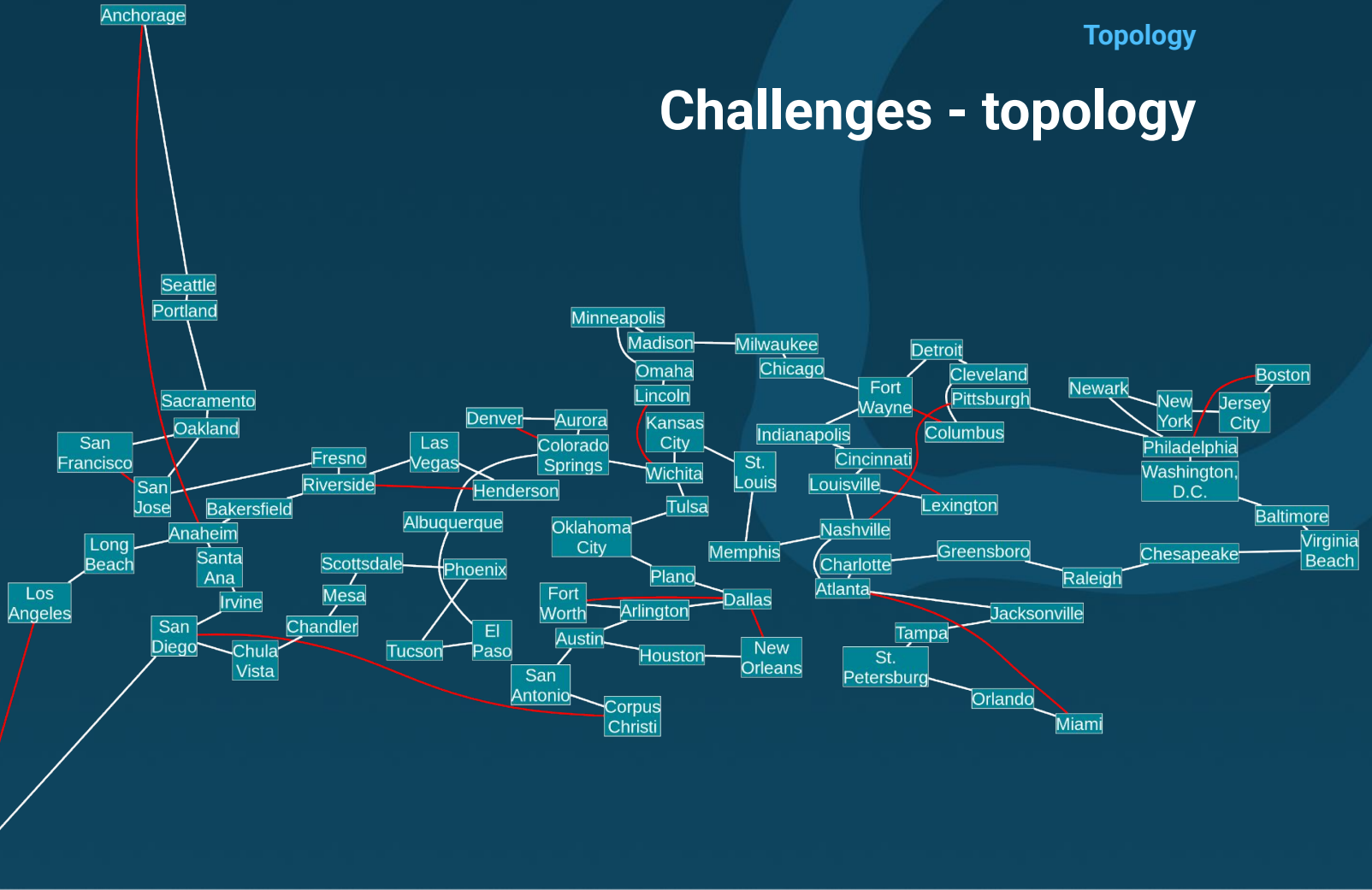
Challenges - topology



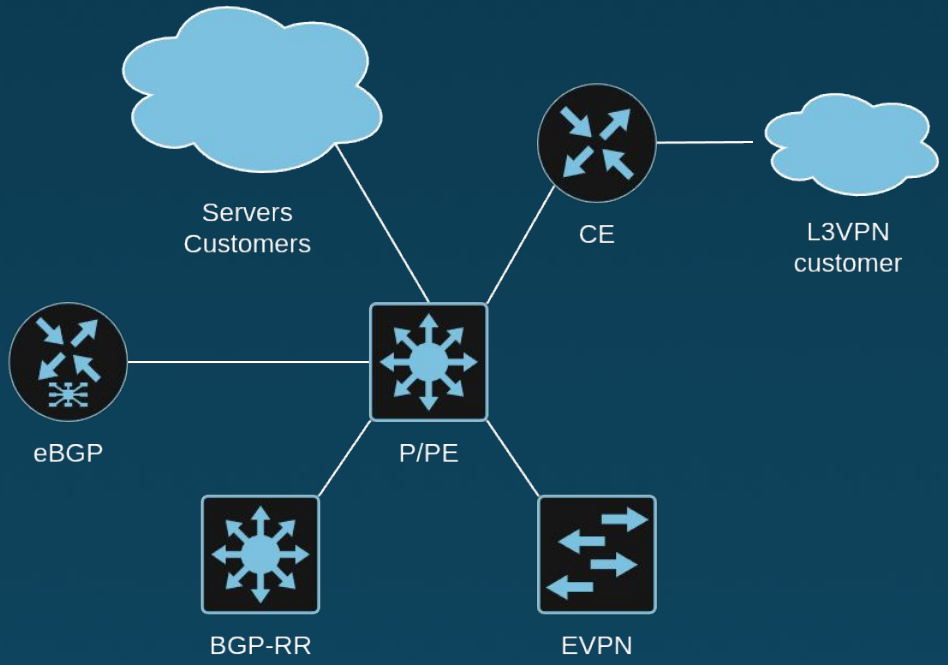
Connection

- No full mesh
- Distance between cities matters
- Redundancy is a must

Challenges - topology



Challenges - devices & services



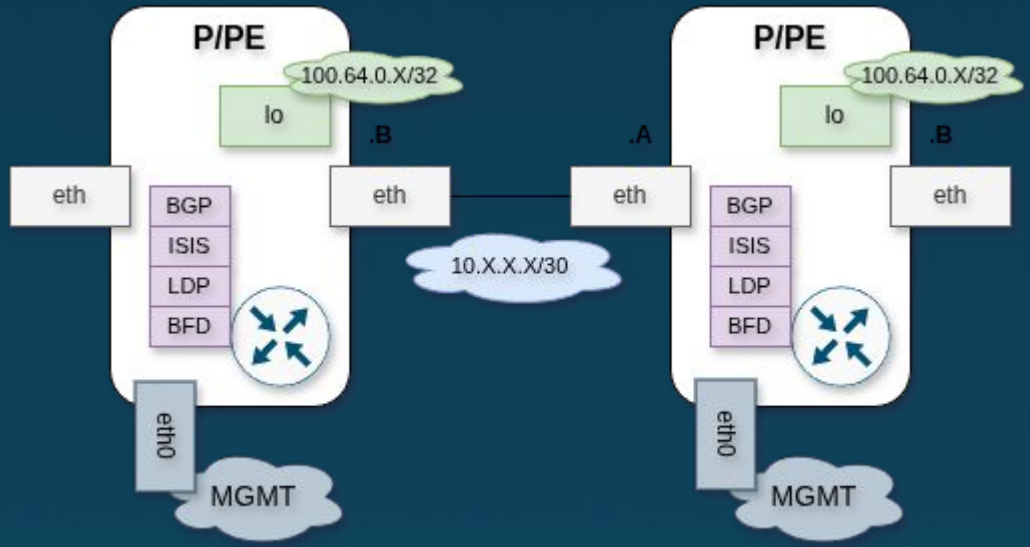
Devices

- 79 x **P/PE**
- 3 x **BGP-RR**
- 3 x **eBGP**

Services

- 35 x **Content**
- 34 x **EVPN**
- 32 x **L3VPN**

P/PE devices



Protocols

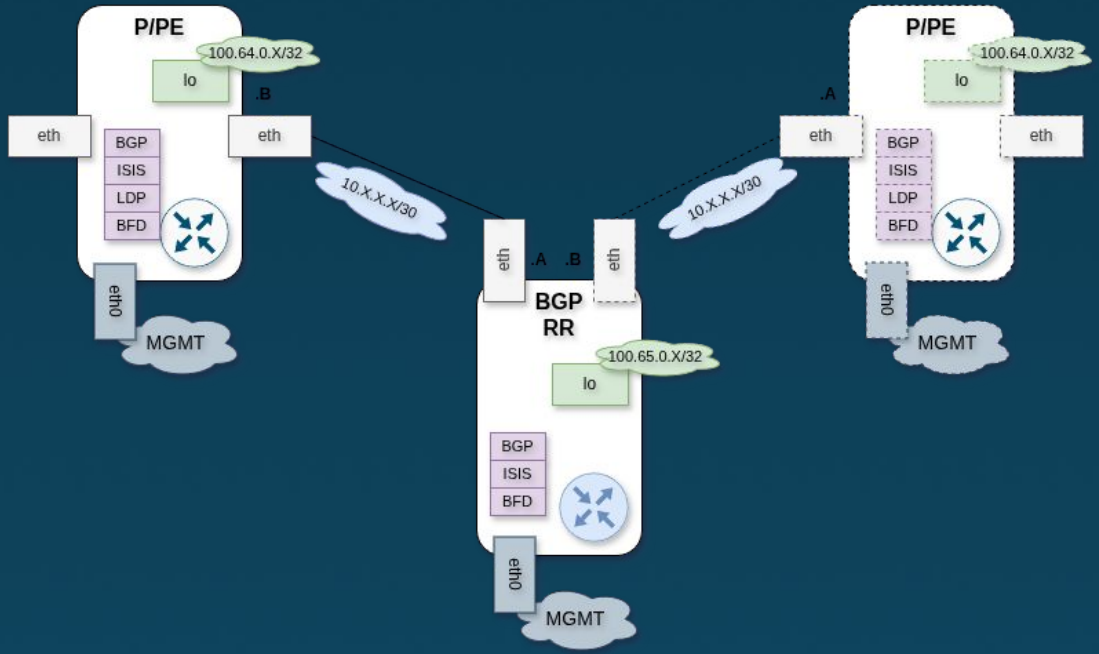
- ISIS, BGP, LDP, BFD
- MPLS for data transport

Purpose

- Provide connectivity between cities
- Connect services to the network

Topology

BGP-RR devices



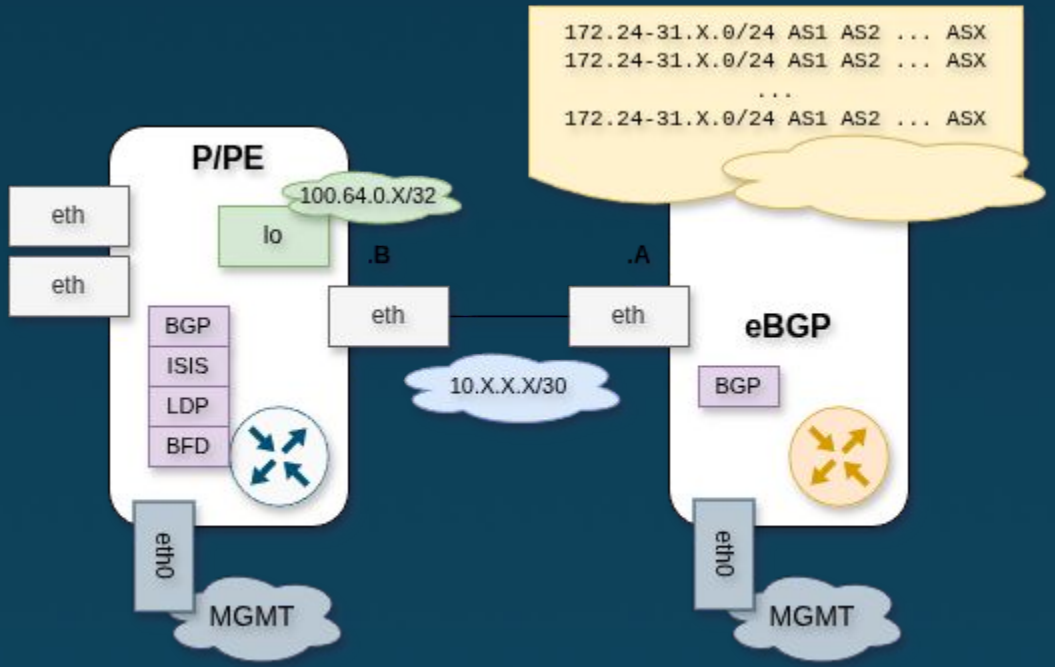
Protocols

- ISIS, BGP

Purpose

- Act as BGP route reflector
- Do not forward traffic

eBGP devices



Protocols

- BGP

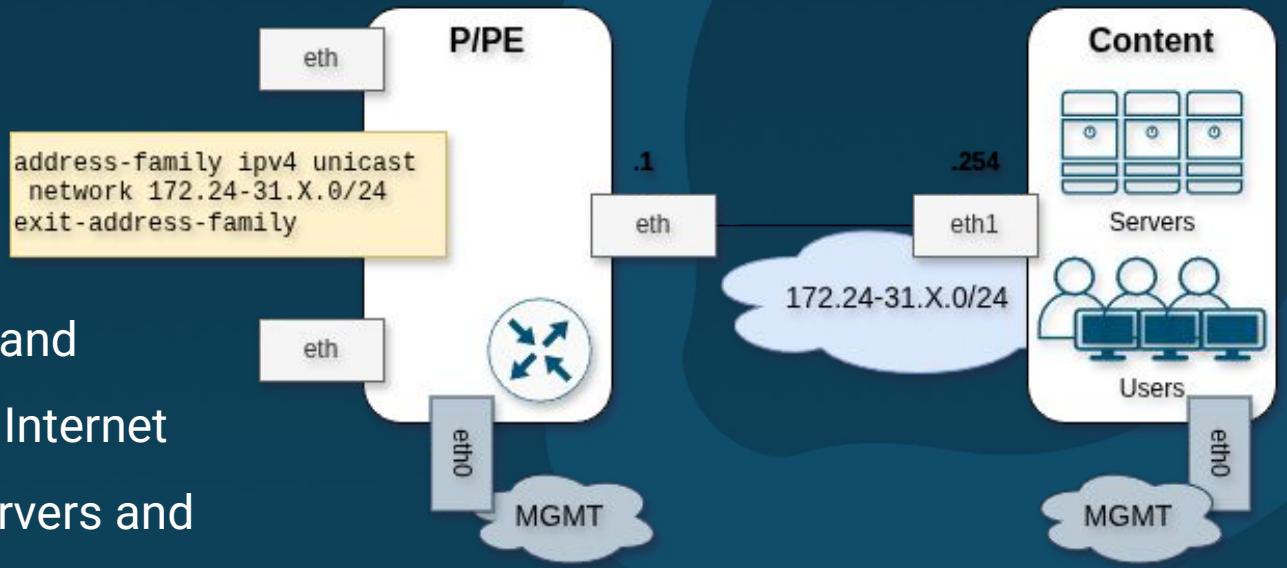
Purpose

- Saturate network with ASes and prefixes

Content service

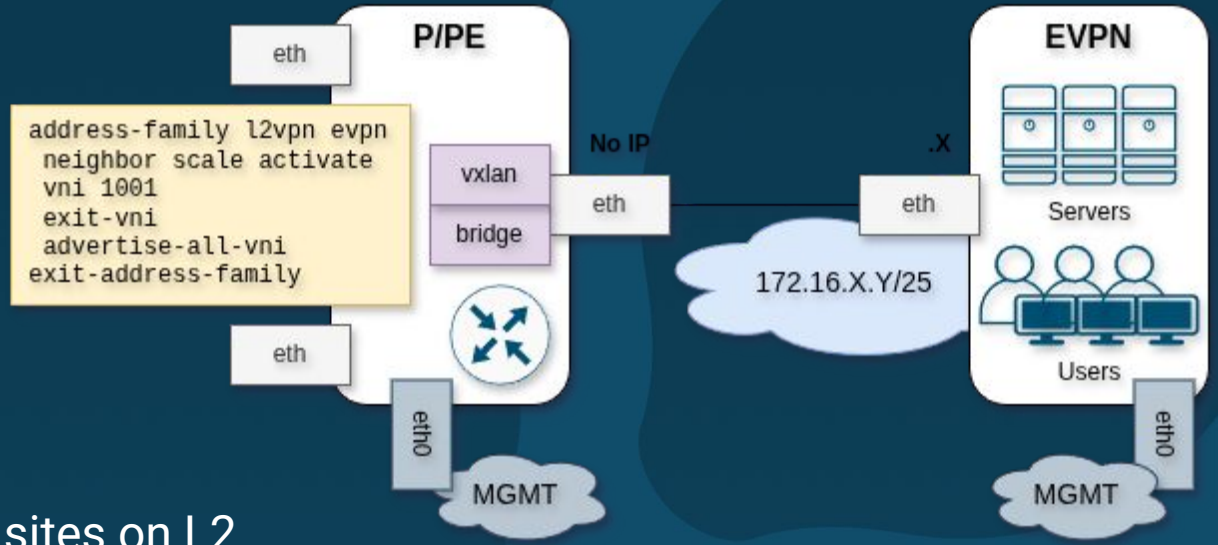
Details

- Emulates servers and customers on the Internet
- Hosts of HTTP servers and clients
- Uses iperf3 to create Internet traffic



Topology

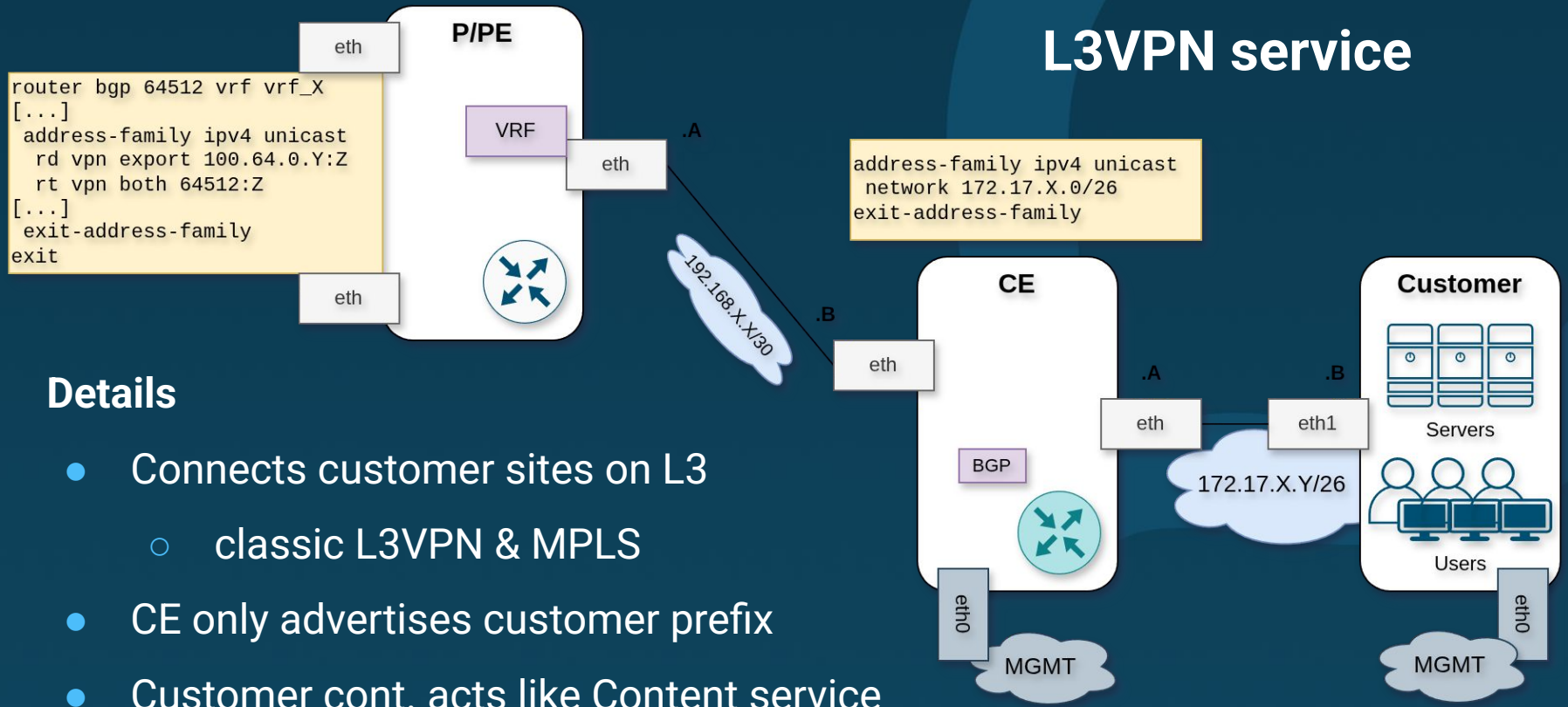
EVPN service



Details

- Connects customer sites on L2
  - Uses EVPN & VXLAN
- Hosts of HTTP servers and clients
- Uses iperf3 to create Internet traffic

L3VPN service



Details

- Connects customer sites on L3
  - classic L3VPN & MPLS
- CE only advertises customer prefix
- Customer cont. acts like Content service
  - Traffic isolated from Internet

Miscellaneous

Additional settings

- Longer BFD timers - to increase BGP stability
- ISIS Fast ReRoute and MPLS Segment Routing
  - Longer ISIS SPF - to lower CPU usage
  - No MPLS-SR controller
- Disabled MPLS TTL propagation
- `icmp_errors_use_inbound_ifaddr` for traceroute
- VRF for management interface in Container Lab

Miscellaneous

Not used features

- IPv6 (and CGNAT) - to keep things simple
- l2circuit / pseudowire / L2VPN - no easy support in Linux
  - We used EVPN instead
- BFD for ISIS - to reduce CPU and increase stability
- BGP full feed - to reduce CPU during failovers
  - Still larger than context window
- Possible (most likely) others

GUI

Introduction to Net-Inspector (demo)

- GUI overview
- Chat and its settings (LLM selection)
- Chat response and AI-agent query processing details
- Topology
- MCP tools

UI demo

Exercises

Introduction: Objectives

- Get familiar with available tools
- Take a look on query execution details to get a feel how AI-Agent is trying to help you
- Experiment with consecutive runs
  - they might provide other results
- Experiment with different LLM models
  - there might be big differences in output and query processing times
  - contrary to last year, LLM models do change a lot

Introduction: Warnings

- If the Net-Inspector App crashes Reload the page (Ctrl+R) should help
- Please wait till query is processed (max 2 minutes)
  - Due to the nature of Streamlit, any UI interaction (e.g. moving map) will stop AI query processing
  - This might have undesired effects on Application
- AI interaction is running without history, every question is independent
- More precise queries increase the chance for valuable output
  - Each word in the query may change the output
- Do not be surprised when even large context window of LLM is exceeded
  - GPT 5 models has much smaller context window that 4.1 (0.4M vs 1M)

Introduction: Example queries to chat

- give me a detailed classification or specific node types from the topology
- review nodes names and tell me naming convention used for nodes in this network topology
- review links and tell me naming convention used this network topology
- show me system versions of nodes: Boston, Content-Boston, CE-4-Boston, CE-IP-4-Boston, RR-Phoenix, EVPN-1-New-York
- show me nodes of customer ‘Apocalypse Inc.’
- show me EVPNs nodes of LexCorp
- show me customers with CE devices and list their node ids

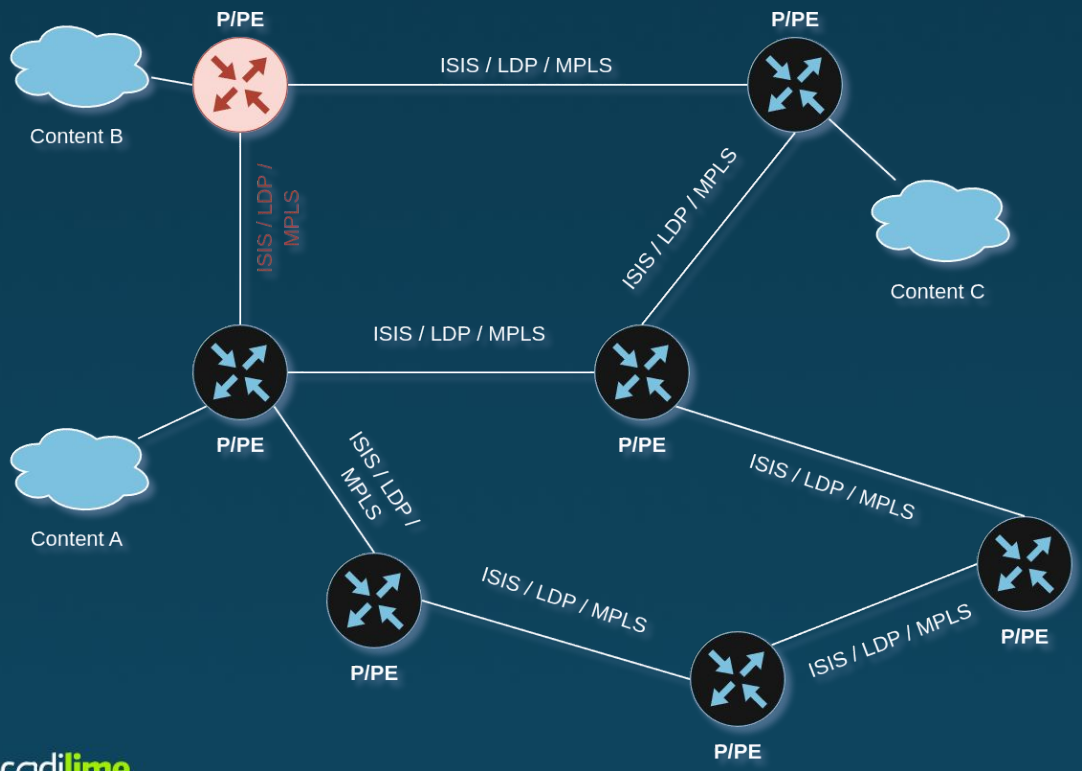
Deadline:

3:20PM

Introduction

Q & A

Task 1a: Topology investigation



Changes

- Removed LDP / ISIS configuration
- Keep link and IP address intact
- Keep SOT intact
- No logs available (yet) to LLM

Task 1a: Objectives

Objectives

- Debug the lack of IGP/LDP redundancy issue
- Find nodes that in terms of IGP/transit traffic has a single path to the rest of the network

Deadline:

3:35PM

Task 1a: Example prompts

- What are the P-PE nodes in the network that have only a single active ISIS neighbour?
- Are there any p-pe nodes without lfa redundancy?
- Are there any interfaces on p-pe devices that have 0 isis active neighbors?

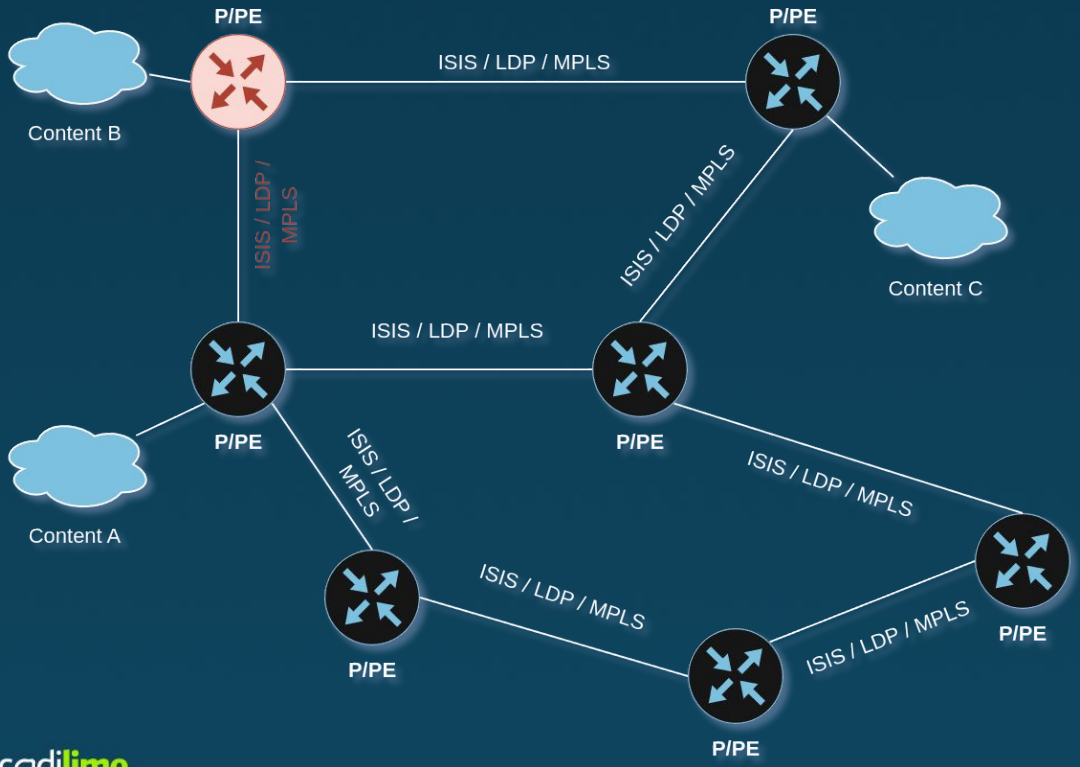
Deadline:

3:35PM

Task 1a: Summary

Q & A

Task 1b: Topology investigation (with Syslog)



Changes

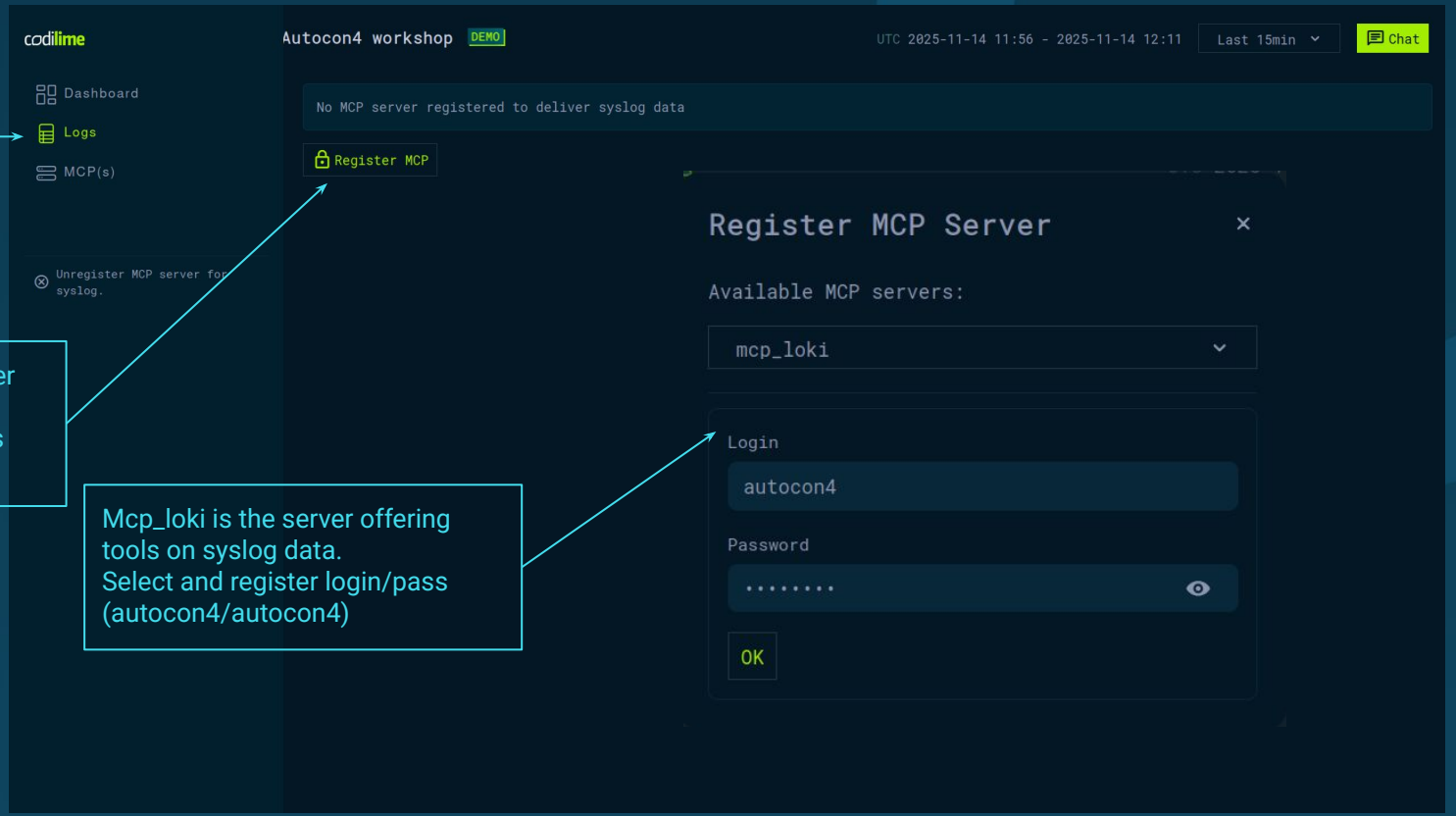
- Removed LDP / ISIS configuration
- Keep link and IP address intact
- Keep SOT intact

Task 1b: Registering MCP

Switch to Logs panel

Initially MCP server for syslog is not available (requires user registration)

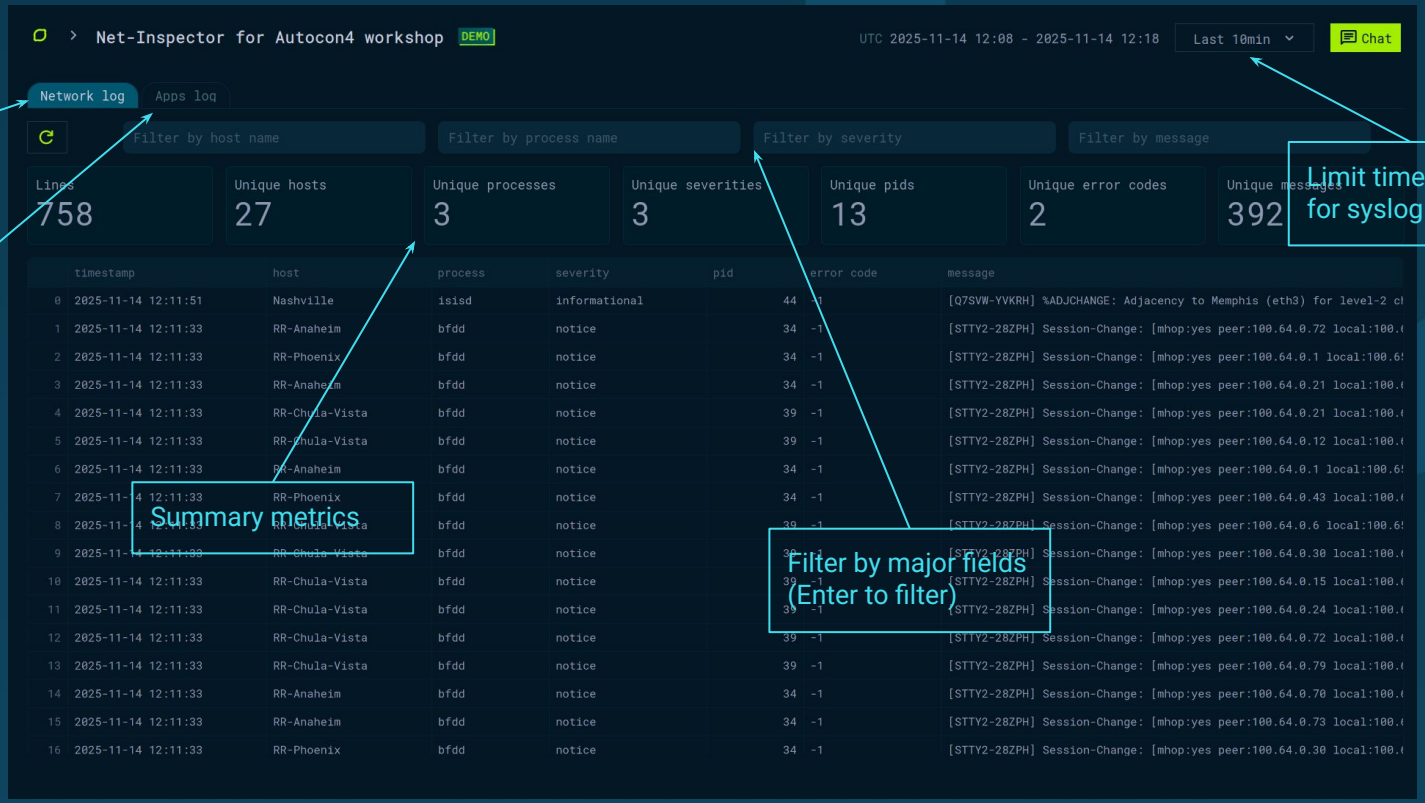
Mcp_loki is the server offering tools on syslog data.
Select and register login/pass (autocon4/autocon4)



Task 1b: Viewing logs

Syslog from network devices

Syslog applications (nginx)



Summary metrics

Filter by major fields (Enter to filter)

Limit time period for syslog data

Task 1b: Objectives

Objectives

- Enable logging MCP
  - Exact steps are in the manual and on next slides
- Find nodes that recently experienced IGP/LDP events received from the network

Deadline:

3:45PM

Task 1b: Example prompts

- Are there anything in the syslogs for the last 20 minutes about isisd on P-PE devices?
- Give the names of the p-pe nodes where isis has changed its state from up to down in the last 10 minutes

Deadline:

3:45PM

Task 1b: Summary

Q & A

Coffee break till

4:15PM

Task 2: Traffic volume drop

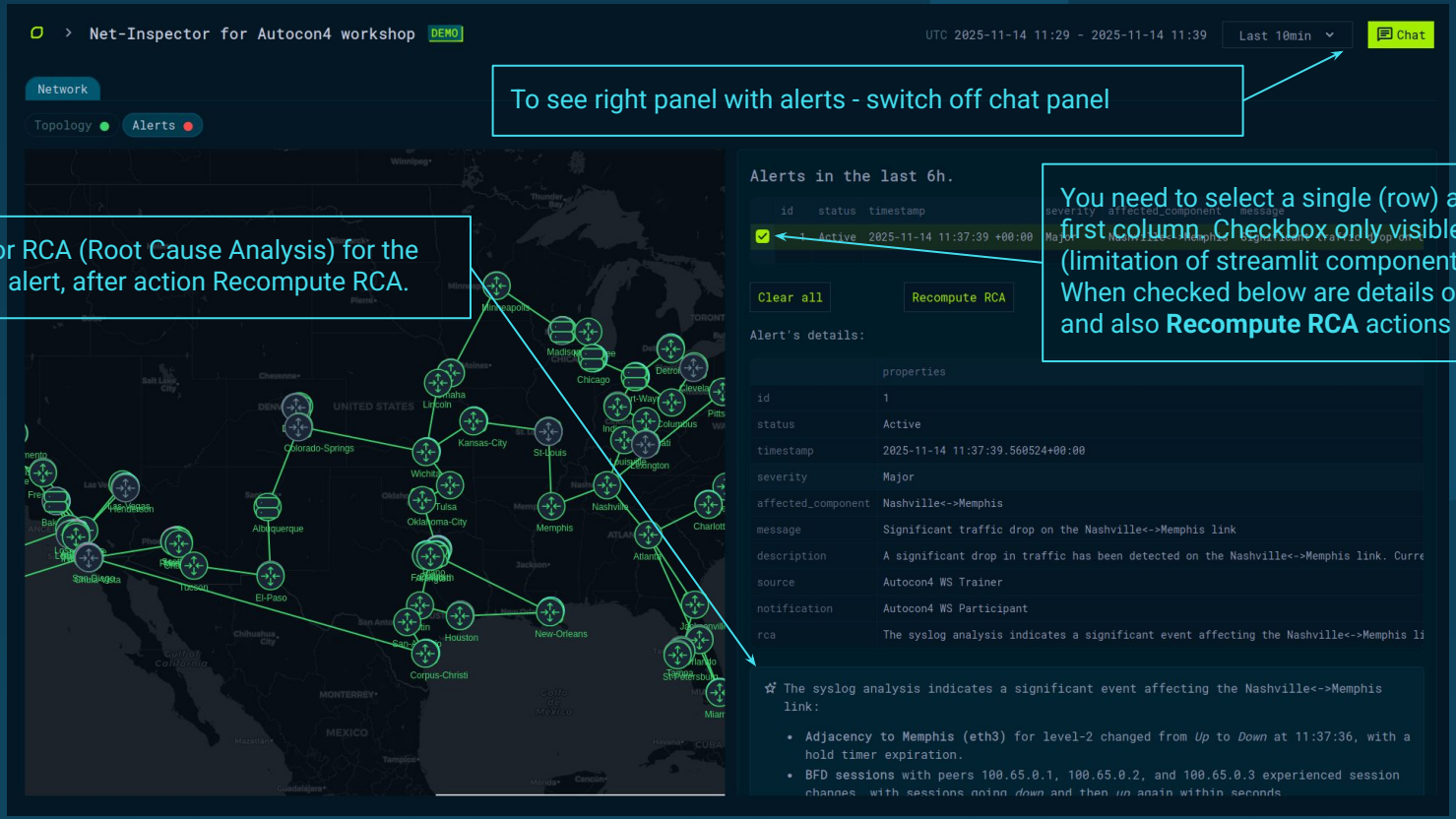
Objectives

- Investigate sudden drop in traffic between two cities
- Get familiar with Alerting and RCA in the UI

Deadline:

4:45PM

Task 2: Using alerts



Task 2: Example prompts

- What is the link status and statistics between Memphis and Nashville devices?
- Run ping test between Nashville and Memphis routers, both directions

Deadline:

4:45PM

Task 2: Summary

Q & A

Task 3: High CPU utilization on P/PE router

Objectives

- Investigate higher CPU utilization on one of P/PE routers
- Find the underlying cause

Deadline:

5:05PM

Task 3: Example prompts

- What is the reason behind the alert about high CPU utilization on one of the devices?
- What may be the reason for Dallas router has high CPU utilization for the bgpd process?
- Is there any bgp instability on Corpus-Christi?

Deadline:

5:05PM

Task 3: Summary

Q & A

Task 4: Internet traffic issues towards selected IP

Objectives

- Find the underlying reason why users in selected cities cannot access site: http://172.30.245.254

Deadline:

2:10PM

Task 4: Example prompts

- Users from Honolulu have the web server at 172.30.245.254 in the Aurora site is respond with HTTP 403. Other sides can access the web server correctly. The problem for sure is with the network. Can you find the root cause of this issue?
- There is something unusual with the 172.30.245.0/24 prefix being advertised in the network. What can it be?
- show route 172.30.245.254" from San-Francisco and Chicago with all the details. Compare them

Deadline:

2:10PM

Task 4: Summary

Q & A

Task 5: Breaking things

Objectives

- Experiment with the topology
- This is the last time, the environment will be used so do not be afraid to break it

Deadline:

2:10PM

Task 5: Summary

Q & A

MCP and AI-agentic apps

Key benefits that the advent of MCP brings

- Better LLMs supporting tool-calling with a standard MCP tool description
- Clear separation between AI-agent development and the management of MCP servers/clients
- User-authentication and authorization built into tool access
- Dynamic modification of AI agents that discover and select MCP tools at runtime
- Stateful, bi-directional interactions between AI-agentic app and MCP server

Better LLMs supporting tool calling

Key benefits that the advent of MCP brings

MCP standardizes tool description
(name, description, arguments and output schema)

LLM providers could better train the models with tool-calling decreasing level of mis-calls

Before MCP
- LLMs with high rates of improperly parametrized tool calls

LLM vendor A

LLM vendor B

...

LLM vendor C

After MCP
- LLMs parametrize tool calls much better

MCP 1

MCP 2

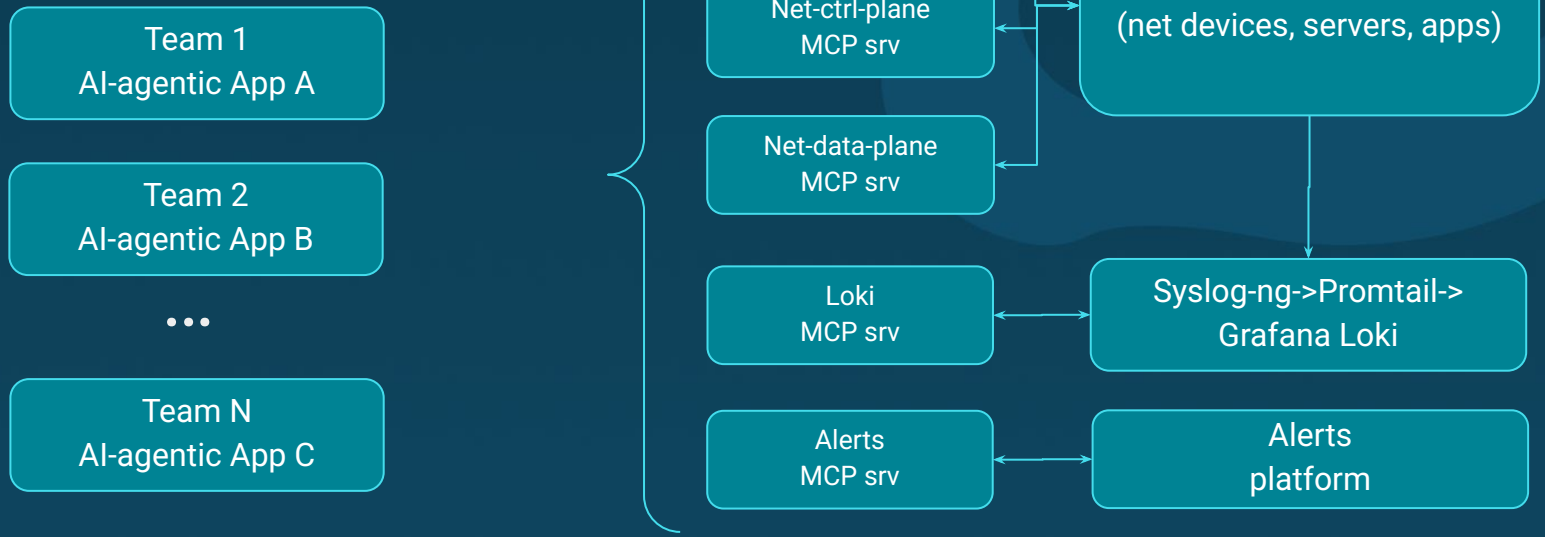
MCP 3

...

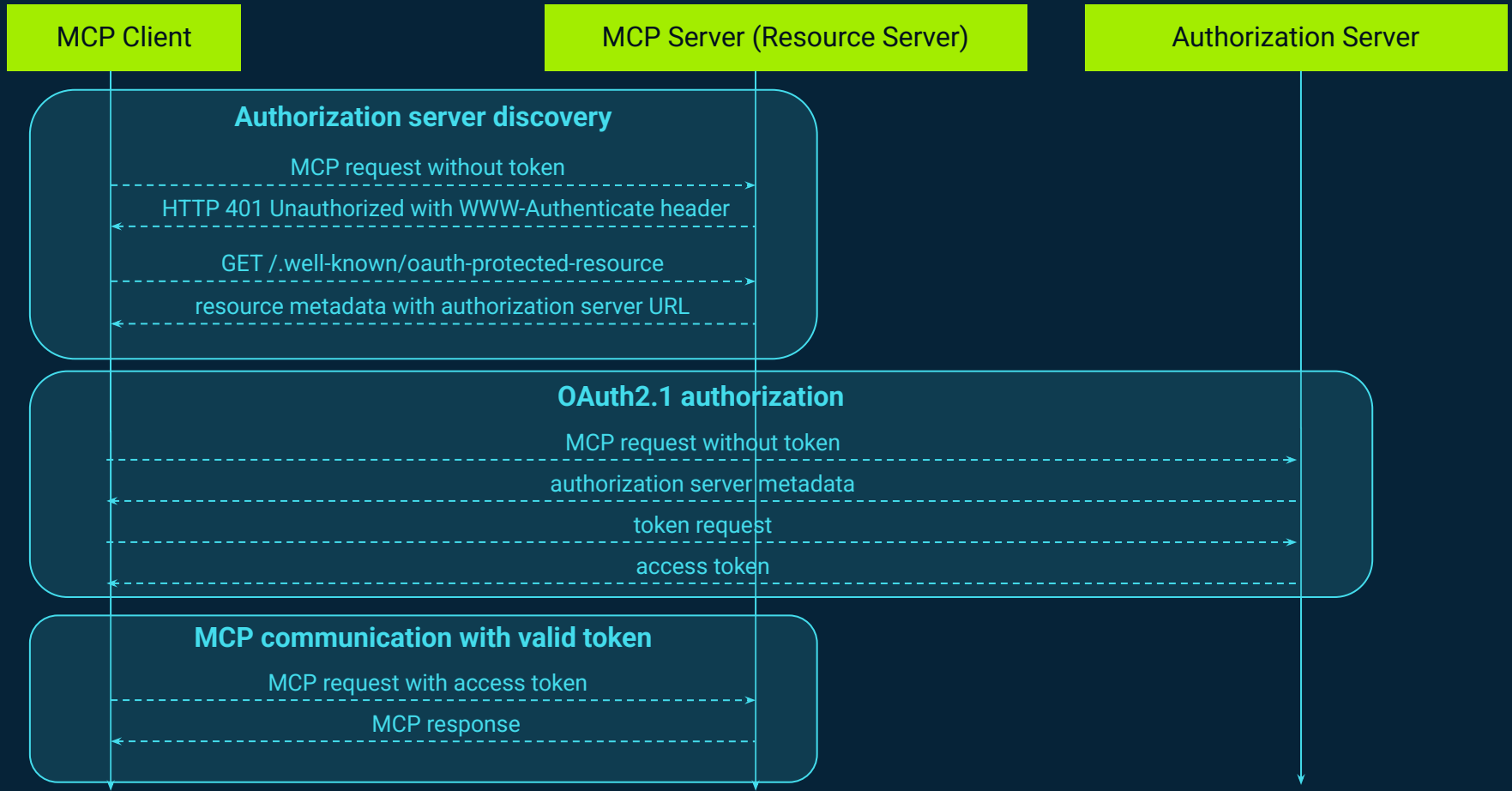
MCP N

Key benefits that the advent of MCP brings

Unified access to resources/tools for LLMs and agentic apps



User-authentication and authorization built into tool access



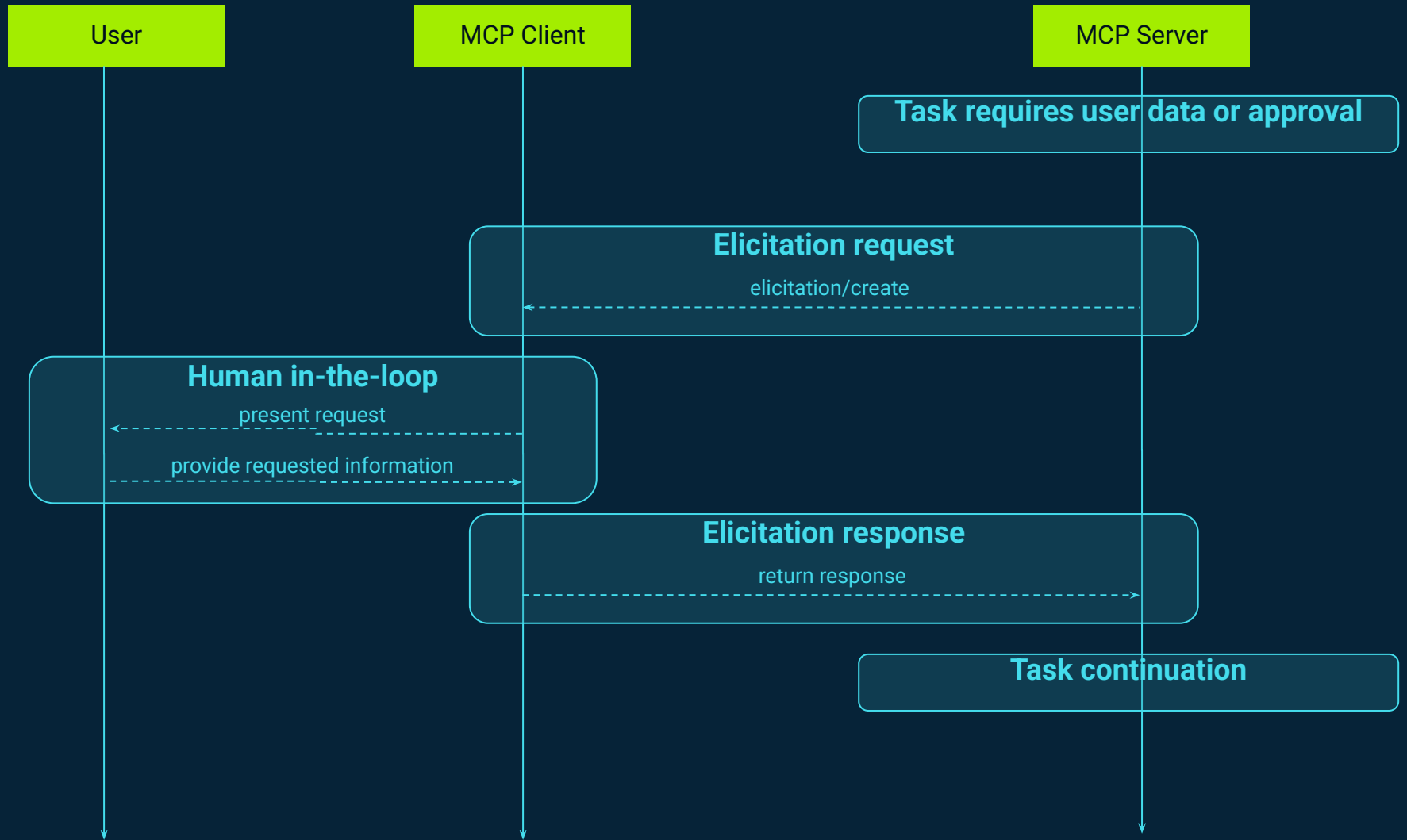
Key benefits that the advent of MCP brings

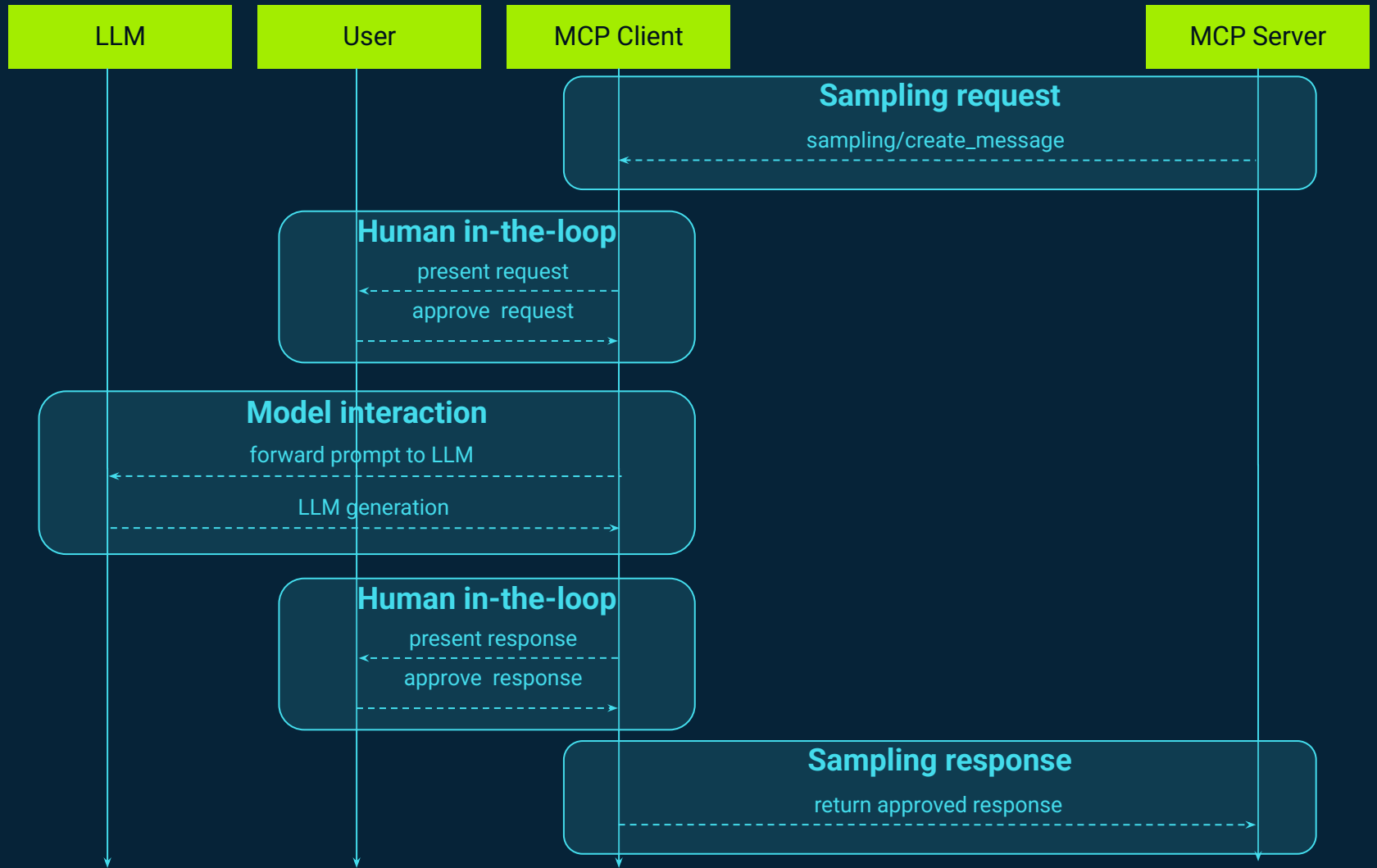
- Notifications via SSE when the available MCP tool list or resources change.
- AI-agentic app can trigger RCA when new alert appeared
- AI-agentic app can modify AI agents adding changed tools dynamically (if we trust MCP provider)
- AI-agentic app can modify AI agents adding a new tool dynamically – but should they?

Stateful, bi-directional interactions between AI-agentic app and MCP server

Key benefits that the advent of MCP brings

- Elicitation
  - allows an MCP server to pause a task and ask the user (through the client) for missing or additional information via a structured prompt (e.g. acceptance for a network command changing the configuration)
- Sampling
  - enables the server to request direct completions or decisions from the LLM (through the client) as part of a larger workflow, effectively placing the client/agent in control of invoking the model for specific tasks (e.g. analyze the syslog errors over the last 10 minutes).


User
MCP Client
MCP Server
Task requires user data or approval
Elicitation request
elicitation/create
Human in-the-loop
present request
provide requested information
Elicitation response
return response
Task continuation


LLM
User
MCP Client
MCP Server
Sampling request
sampling/create_message
Human in-the-loop
present request
approve request
Model interaction
forward prompt to LLM
LLM generation
Human in-the-loop
present response
approve response
Sampling response
return approved response

Challenges of MCP for AI-agentic apps

- LLM supported AI-agents are very sensitive to tools' descriptions
  - MCP server developer need to refine description according to needs of AI-agentic app teams
- Complex logic in stateful session management (especially for autonomic AI-Agents)
  - when interactions are required between User<->AI-Agent<->MCP-client<->MPC-server
- Harder debugging
  - But MCP protocol requires to provide status of tool execution and error/exception messages at MCP server side

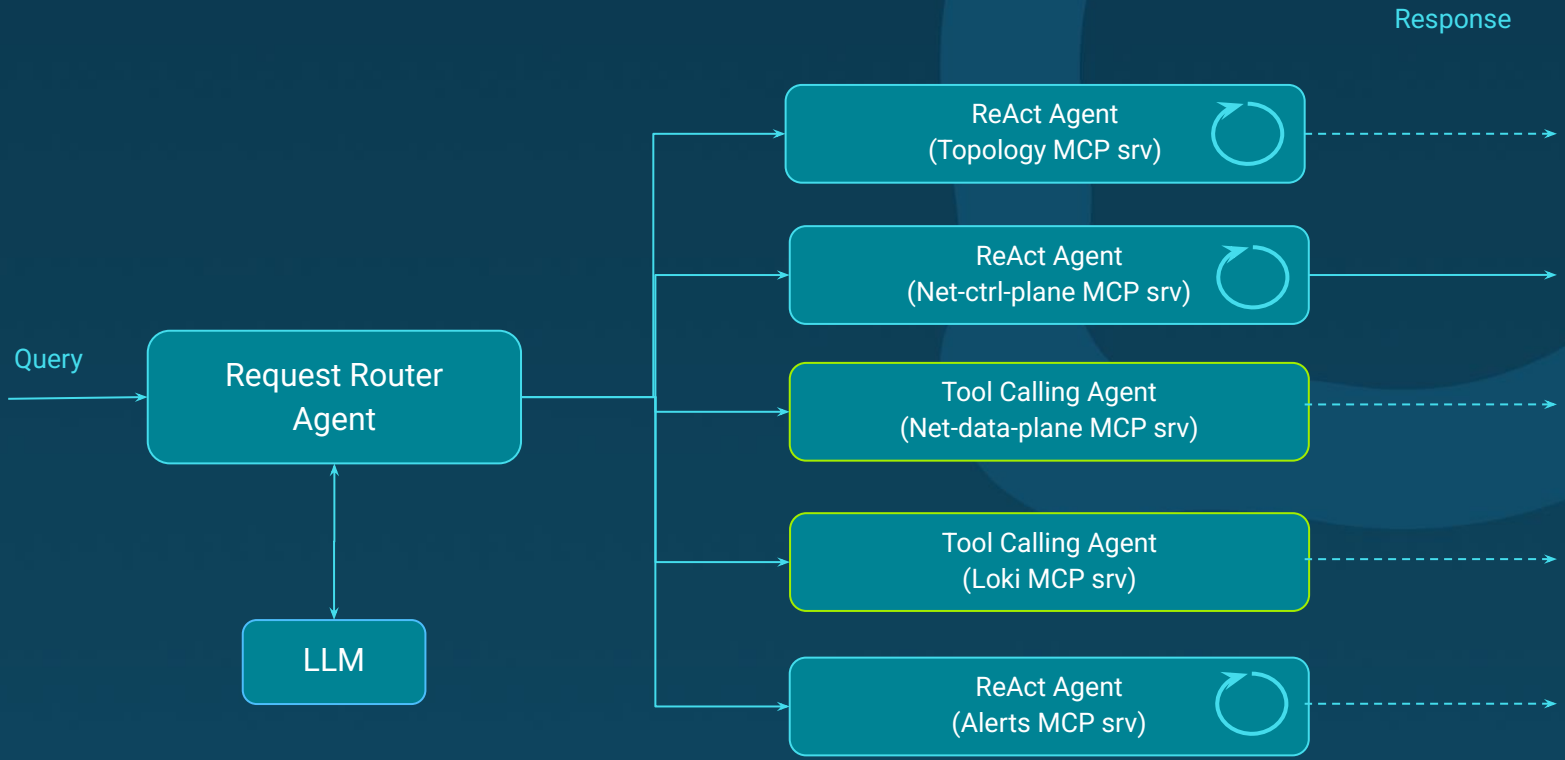
Discussion

How to build valuable AI-agents in networking domain

- Proper multi-agent architecture
  - Request Router, Coordination Agent, LangGraph workflows as tools …
- Experience and intuition how AI-agents work and utilize MCP tools
- Super important tools’ descriptions (network experts vs MCP developers)
- Automatic e2e testing using specialized frameworks/libraries
  - Against various LLMs
  - Collection of ‘golden answers’ (feedback loop)
  - LLM as a judge
- Inter-domain team and collaboration

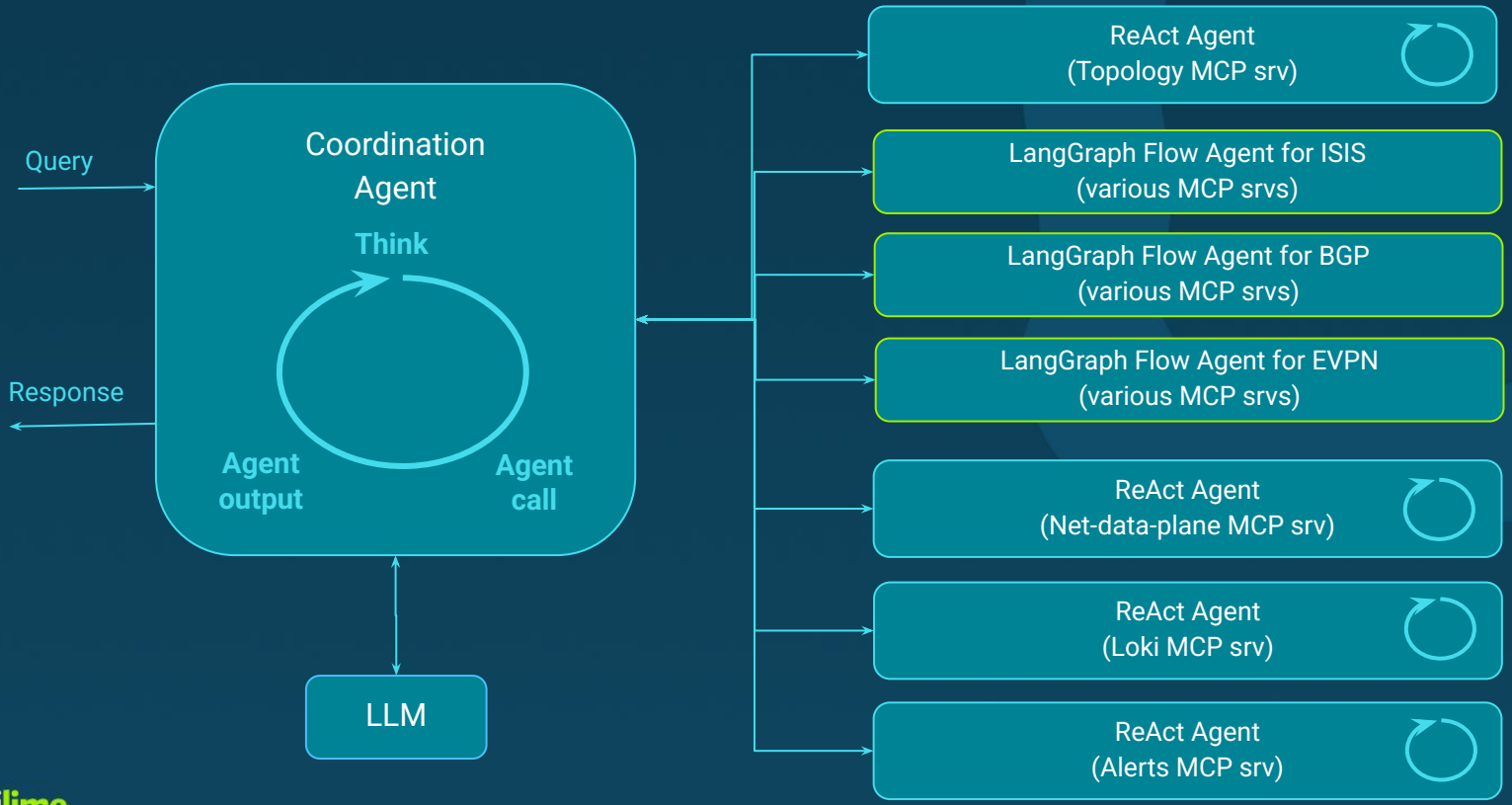
Discussion

Key multi-agent architectures



Discussion

Key multi-agent architectures



Summary

Summary

Workshop summary

- Chance to try AI to solve problems in large, complex network topology
- Gained familiarity with the ReAct agent, various LLMs, and MCP server tools
  - including the role of the MCP protocol in agentic applications.
- Observed the maturity and limitations of LLMs and the agentic framework
  - multi-agent architectures that can mitigate these drawbacks.

Workshop summary

We would like to say that ai-agentic applications utilizing MCP servers are simple and we can easily apply AI for plethora of tasks related to networking infrastructure

But they are **NOT**.

Building reliable ai-agents requires highly skilled engineers closely cooperating with network engineers.

Estimated workshop cost

	GPT-4.1 mini	GPT-4.1 nano	GPT-5 mini	GPT-5 nano
Price for 1mln INPUT tokes	**$0.40**	**$0.10**	**$0.25**	**$0.05**
Price for 1mln OUTPUT tokes	**$1.60**	**$0.40**	**$2.00**	**$0.40**
Avg. question time	**30**	**20**	**60**	**40**
Question cost	**$0.05**	**$0.01**	**$0.05**	**$0.01**
Worst case scenario cost	**$1,123.20**	**$421.20**	**$526.50**	**$157.95**
Expected cost *	**$234.00**	**$58.50**	**$219.38**	**$43.88**

** with 65 active users and 15 questions per exercise*

Summary

Q & A

Thank You