From Automated to Autonomous: Orchestrating the Network with Agentic AI

HPE Juniper Networking

Aditya Kaul – Principal Architect, Professional Services APJ

Can Agents replace Knowledge workers?



Wrong Question!

Juniper Business Use Only

Augmenting, not Replacing the Knowledge worker

Guardian angel

Discovers and warns you about unanticipated, possibly catastrophic events that could impact your safety, security, and wellbeing



Cognitive amplifier



Anticipates what you want to do and helps you to do it with less effort

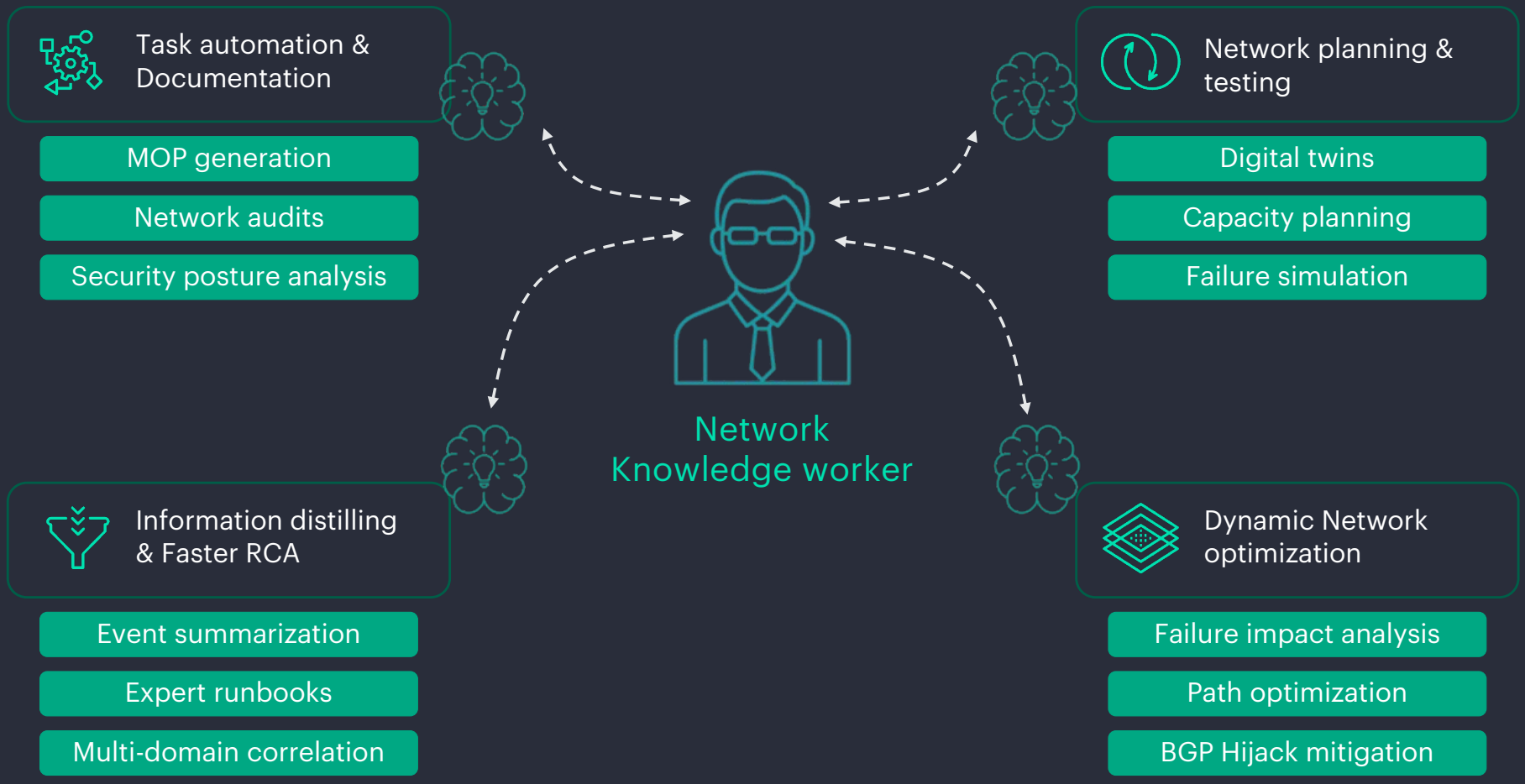


Knowledge worker

Future opportunities lie in creating tools for coping with 21st century world of "too much information and too little time". *... Dr. Raj Reddy, CMU, Turing Award winner*

Juniper Business Use Only

Cognitive Amplifiers for the Network Knowledge Worker

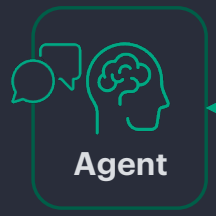


Juniper Business Use Only

Agentic systems: The building blocks

Tuning the system to its environment

Data creates knowledge



Context creates meaning

Fine-tuned LLMs
(Model w/ context)

- Embeds domain-specific knowledge directly into model weights

Real-time streaming
(More data)

- Continuous feed of current system state, sensor data, and metrics

Knowledge RAGs
(Data + Context)

- Retrieves relevant information from indexed knowledge bases
- Gives the agents more context (your secret sauce)

Tools
(Data + Actions)

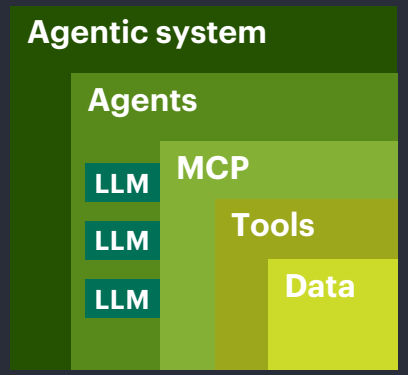
- Connects agents to environment (systems, databases, services)

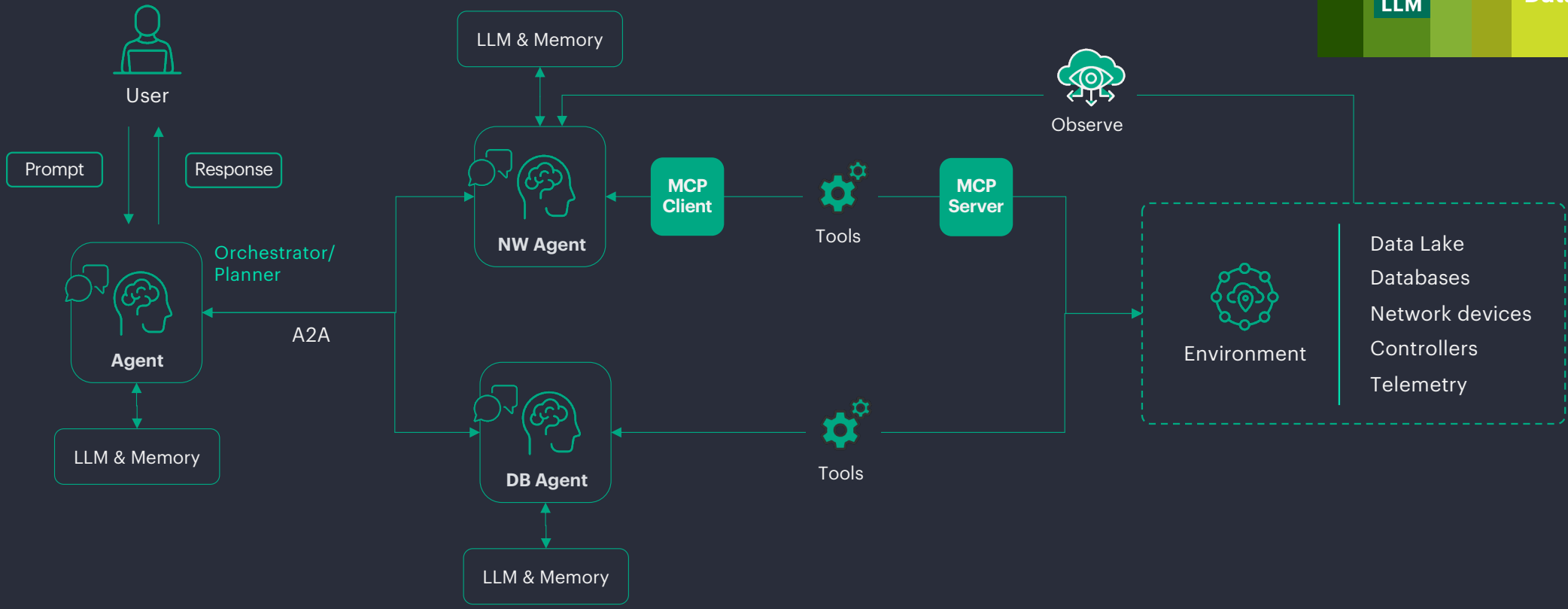
Juniper Business Use Only

Agents & Tools

Beyond traditional AI:

- Agentic AI doesn't just respond—it **plans, executes, and adapts** to achieve complex objectives.
- **A2A & MCP** provide standardized interfaces to integrate custom environments into the LLM's context.
- Agents don't always need A2A & MCP for integration. They can leverage traditional interfaces.





Juniper Business Use Only

UC 1: Network infrastructure Assessment, Config Audit (BGP, SRv6)

Anatomy of an Effective Network Assessment Prompt

Provide Structured Instructions: Guide the AI with a clear, step-by-step process rather than a single, broad command.

Decompose the Objective into Granular Tasks: Break down the high-level goal into specific areas of analysis. For example:

- ISIS Topology & Adjacency Review
- BGP Peering & Policy Audit
- SRv6 Path Validation
- VPN Service Configuration Check
- Summary of Findings & Recommendations

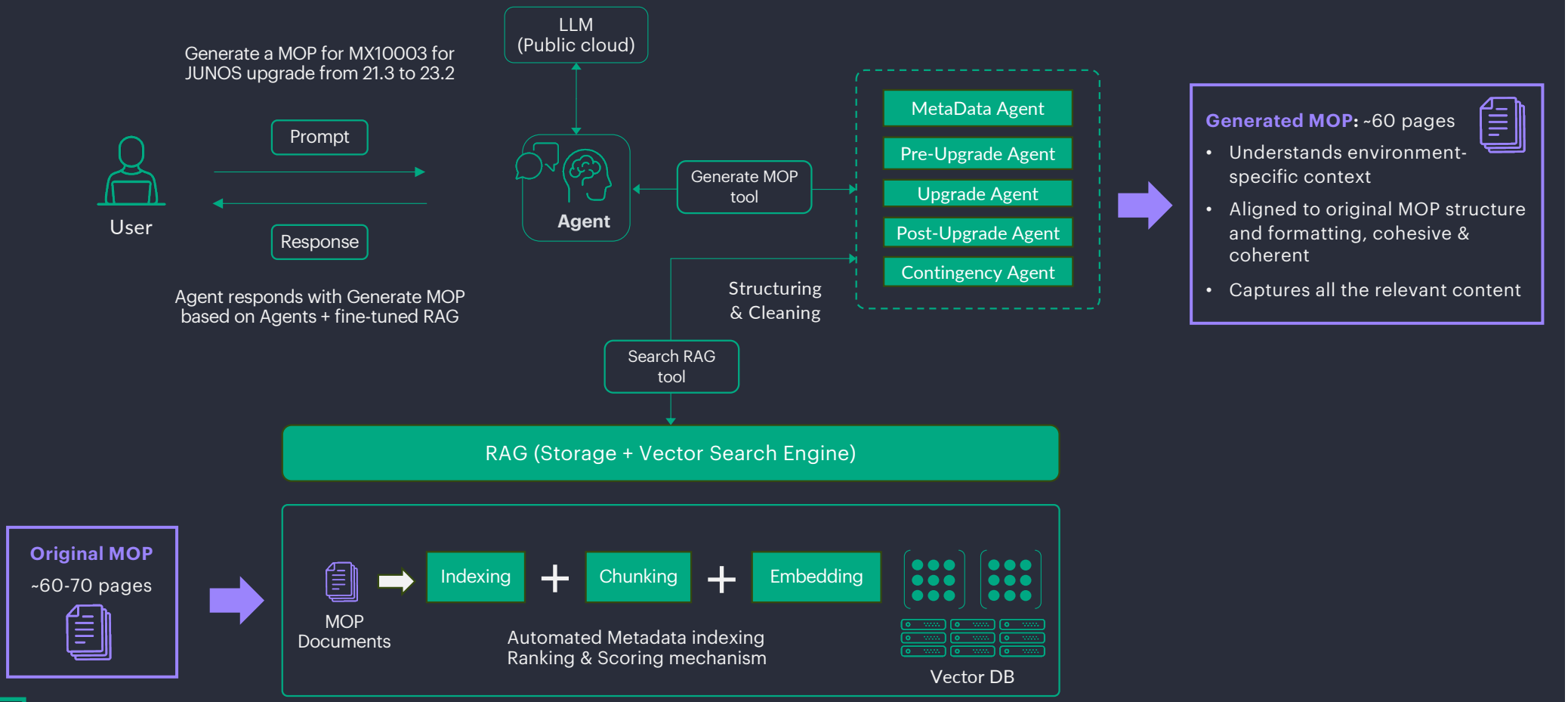
Define Negative Constraints (The "Don'ts"): Explicitly state what the agent must *not* do or include in its output. This is a critical guardrail to mitigate model hallucination and keep the analysis focused.

```
Analyse the entire network by checking the Juniper vMX logical systems in the POP1(192.168.1.221) and POP2(192.168.1.222)
Create an extensive report with graphics, html but tabulation and illustrations , i want to download this report as html.

First chat/prompt should define the Part 1 and 2 subsequently other prompt should finish parts 3 & 4.
Requirements:
1. Detailed graphical topologies showing all nodes and how they're connected
2. OSPF Database and  ISIS database details with ISO addressing with realtime examples.
3. Loopback addressing information
4. iBGP and eBGP peering diagrams (including Internet peering)
5. Route Reflector connection and BGP topology visualisation
6. PDF-ready format
Part 1 will include:
* Executive summary and overall network health
* Detailed ISIS topology with ISO addresses
* ISIS database visualisation
* SRv6 infrastructure deep dive with locator topology illustration
Part 2  will include:
PART 2: Routing Protocol Analysis (Next Chat)
  ├── BGP peering topology & route reflector mesh
  ├── iBGP/eBGP relationships & external connectivity
  ├── Performance metrics & convergence analysis
  └── Traffic distribution & ECMP analysis
  please add more details on the internet part, as-path visualisation, the analysis of various prefixes
Also show the entire BGP community structure with policies and mention the community and local-preference.

Part 3  will include:
* VRF services detailed analysis
* Flex-Algorithm 128 deployment details
Part 4 will include:
* Issues and remediation plans
* Recommendations and conclusions
```

Juniper Business Use Only

UC 2: MOP generation

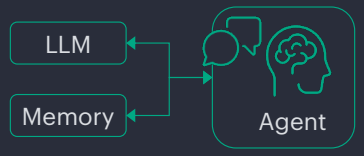
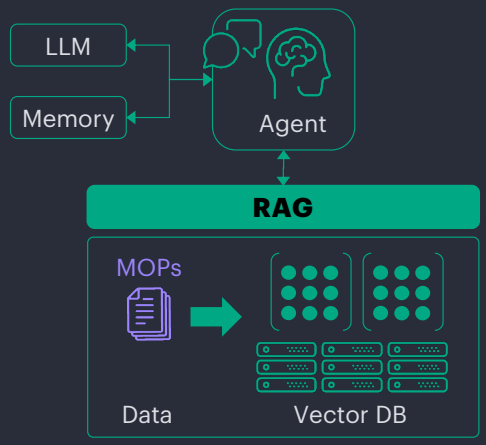
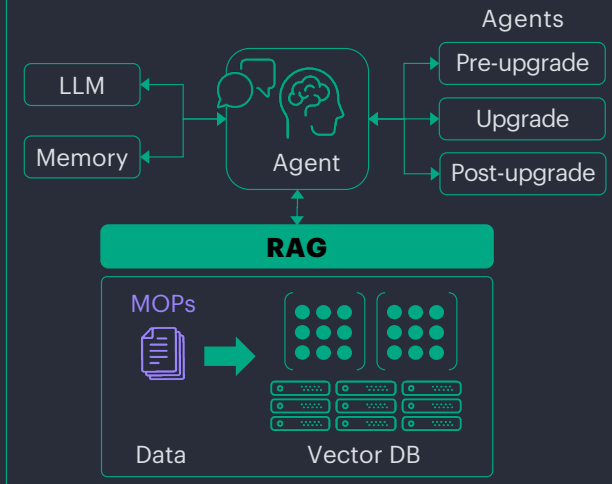
Inference + Multi agent + Fine-tuned RAG



Juniper Business Use Only

Why RAG & Multi-agent?

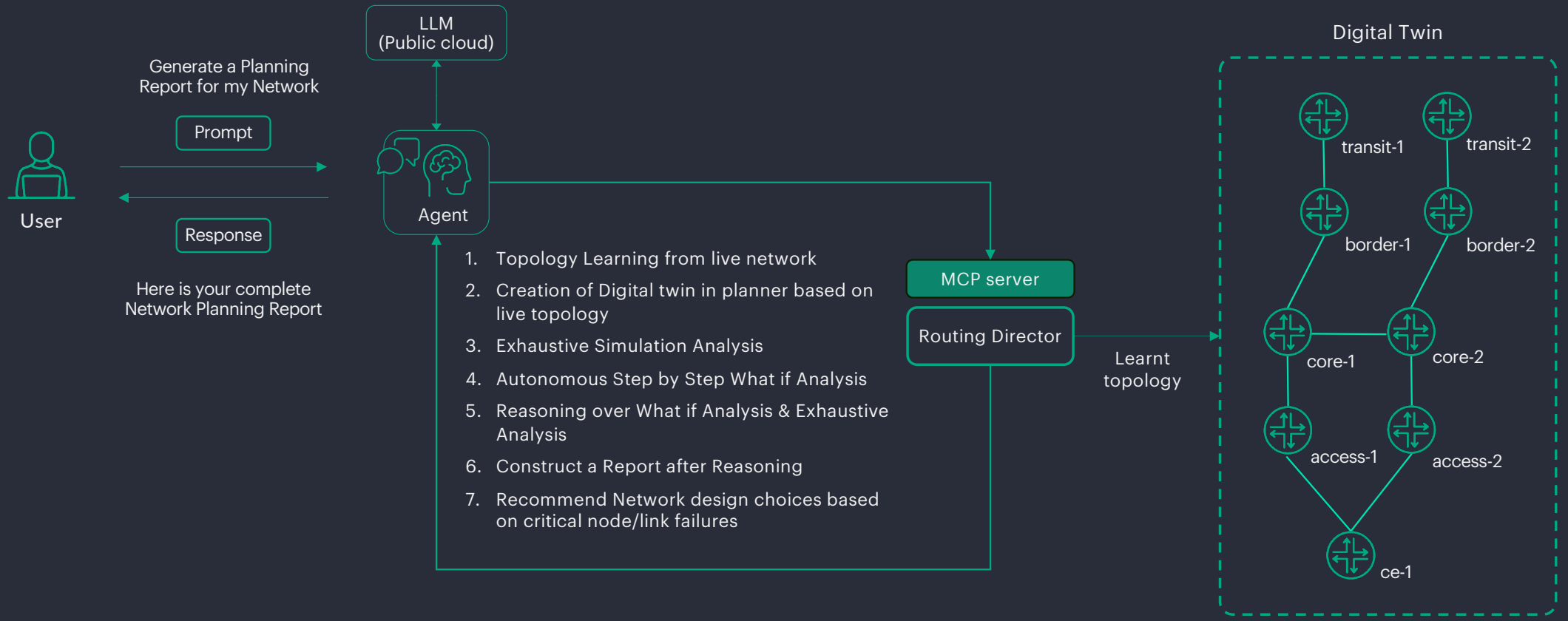
Original MOP: ~60-70 pages

	Inference only (no RAG, LLM fine-tuning or multi-agent)	Inference + RAG (no LLM fine-tuning or multi-agent)	Inference + RAG + Multi-agent (no LLM fine-tuning)
Setup			
Result	**Generated MOP:** • 11 pages • Generic MOP based on LLM's previously learnt knowledge • No environment-specific context	**Generated MOP:** • 278 pages • Understands environment-specific context • Poorly structured, not coherent & cohesive	**Generated MOP:** • ~60 pages • Understands environment-specific context • Aligned to original MOP structure and formatting, cohesive & coherent • Captures all the relevant content

Juniper Business Use Only

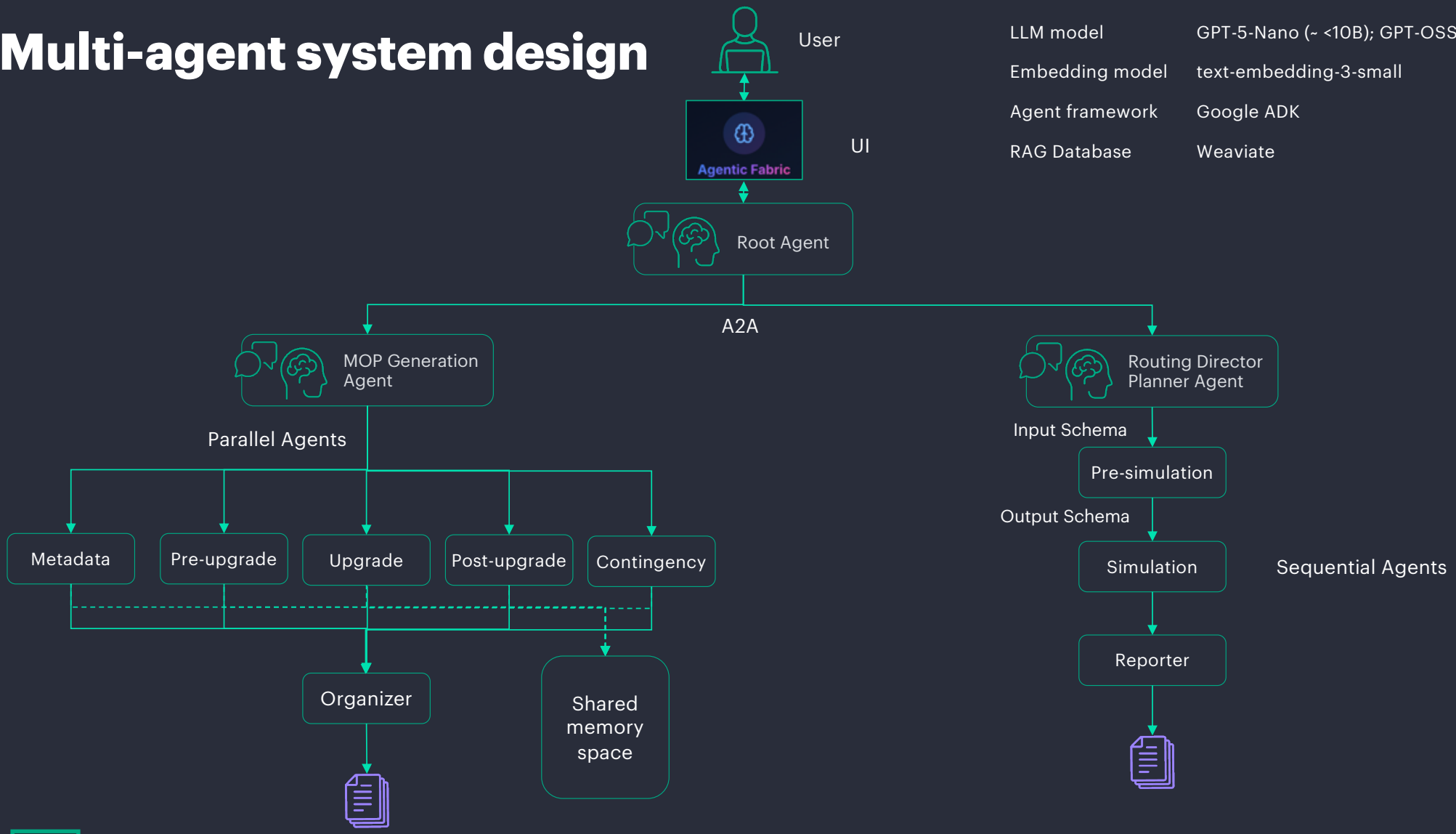
UC 3: Network capacity planning

Failure simulation and What-If analysis



Juniper Business Use Only

Multi-agent system design



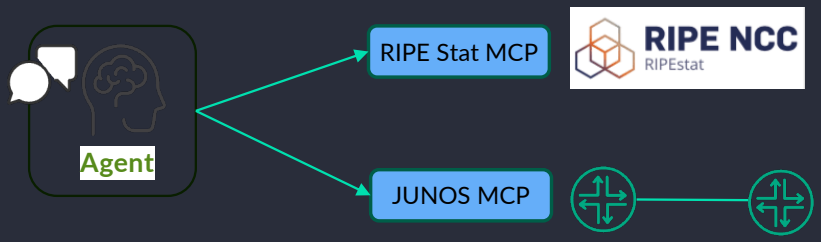
LLM model	GPT-5-Nano (~ <10B); GPT-OSS-20B
Embedding model	text-embedding-3-small
Agent framework	Google ADK
RAG Database	Weaviate

Juniper Business Use Only

UC 4: BGP Route hijacking

Leveraging External Intelligence for BGP Analysis to mitigate issues like Route Hijacking

- **Integrates with Authoritative Sources:** The agent autonomously queries public data platforms like Cloudflare Radar and RIPE Stats.
- **Provides External Visibility:** Gains an essential "outside-in" view of BGP routing to validate internal observations.
- **Enables Event Correlation:** Correlates global routing data with internal network events for faster, more accurate root cause analysis.



Critical Finding: This is a Major Issue!

Who Owns 1.1.1.0/24:

Owner: Cloudflare (AS13335) / APNIC Labs
Purpose: Cloudflare's famous public DNS resolver service (1.1.1.1)

This is **one of the most well-known IP addresses on the internet** - Cloudflare's public DNS service!

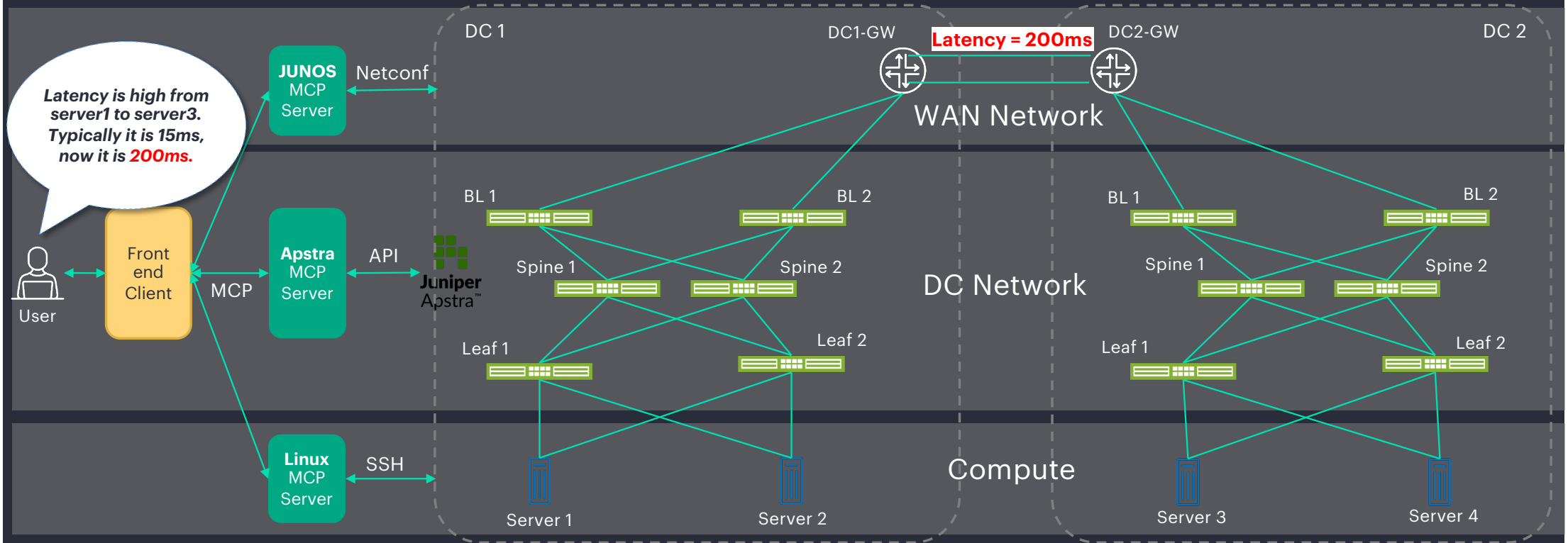
What This Means for Your Network:

This is a SERIOUS Configuration Problem:

1. **IP Hijacking/Route Leak:** Your router B4 is incorrectly advertising Cloudflare's prefix (1.1.1.0/24) as if AS7473 owns it
2. **BGP Hijack Scenario:** When you advertise 1.1.1.0/24:
   - Some networks may route traffic destined for Cloudflare's DNS (1.1.1.1) to YOUR network instead
   - This creates a "blackhole" where DNS queries never reach Cloudflare
   - Users trying to use 1.1.1.1 as their DNS server would fail
3. **Why It's Not Globally Visible in RIPE:**
   - RIPE collectors may be filtering it as an invalid announcement
   - Most networks likely reject this route as invalid (AS13335 is the legitimate origin)
   - Your peer AS 2004 may be accepting it but others are not
4. **Reputation Risk:**
   - This looks like BGP hijacking (even if unintentional)
   - Could result in your network being filtered or blacklisted
   - Violates internet routing best practices

Juniper Business Use Only

UC 5: Multi-domain Root Cause Analysis



Demo scenario:

- User complains that latency is high from server1 to server3
- Typical latency = 5ms, Current latency = 200ms
- Agent troubleshoots the problem to find the root cause

Juniper Business Use Only

The Augmented Network Knowledge Worker

- Document generation
- Digital Twins
- Network Planning
- Audits & Reports
- Security posture check



The Augmented
Network Knowledge Worker

- Cross-domain Orch
- Route validation
- Expert runbooks
- Root Cause Analysis
- Sustainability

Juniper Business Use Only

Thank You

Aditya Kaul (aditya.kaul@hpe.com)

Credits: Thank you co-pilot for augmenting this knowledge worker



© 2026 Hewlett Packard Enterprise Development LP

Juniper Business Use Only