Intelligent Network Troubleshooting Assistant

Tech Con 2025 Abstract 525

HPE Edge;

Intelligent Network Troubleshooting Assistant

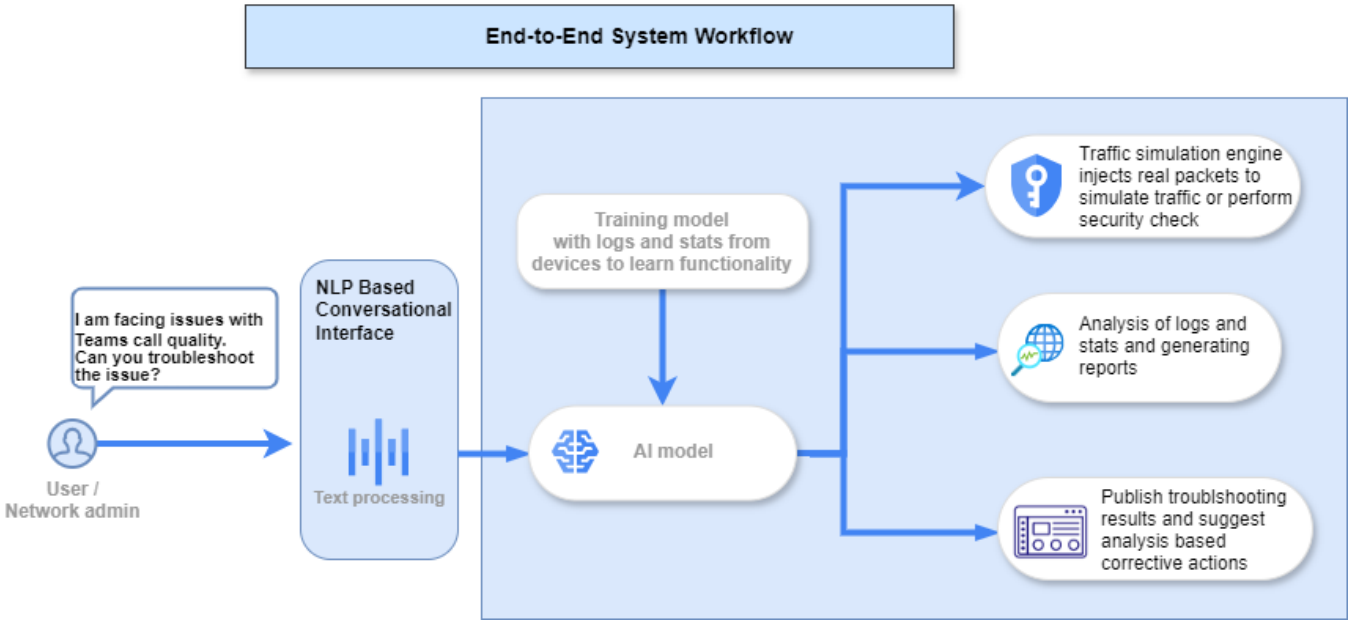
Abstract

The advent of AI/ML technology in networks is becoming increasingly evident as campus networks evolve into more complex systems. AI transforms networking by helping to accurately identify issues and root causes and quickly respond to them in real-time, thus minimizing disruptions. This paper describes an AI based network assistant with Natural Language Processing (NLP) capabilities to perform intelligent network troubleshooting to root cause and troubleshoot network issues with traffic injection mechanism based on user input. Going forward, since network configurations (config management) are also evolving towards NLP based assistant systems, the proposed system could provide the ability to troubleshoot anomalies by isolating specific problems in realtime and also provide feedback for the config management system to take corrective actions accordingly.

Problem statement

More often than usual, network configurations are prone to cause undesirable side effects, requiring additional corrective configurations. This could cause disruptions which are extremely challenging and time consuming to manually root cause and troubleshoot. Sometimes, issues could also be specific to a particular kind of application traffic (such as VoIP). The troubleshooting for such scenarios at times, would require actual traffic to debug the root cause based on outcome at that particular moment. The solution proposed by this paper involves a system with conversational interface (based on NLP) and an AI model trained with packet captures of various applications to intelligently generate traffic that replicates the actual application traffic in the network and provide the troubleshooting results that we can correlate with relevant resolutions. The system could also perform security tests as described by the user to analyze threats that exist with the network.

Our solution



System functionality

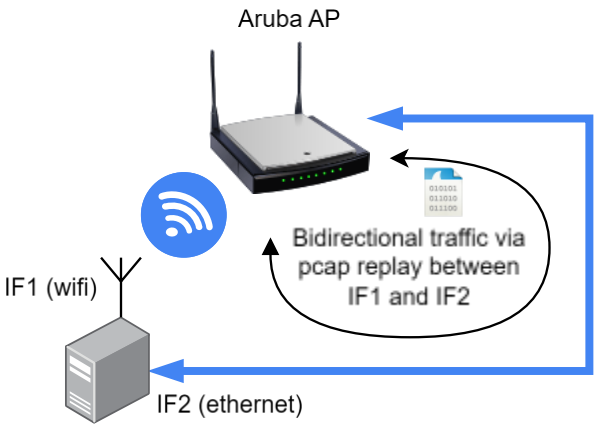
As depicted in the above flowchart, the proposed solution involves an AI-based assistant (that could be running on Aruba Central) which is a system capable of following:

- **Process user description into troubleshooting action item**:

  The AI model would be trained with a language model (like GPT-2 or BERT) to provide a conversational interface with the user. The processed results would determine the exact type of troubleshooting action item to achieve with traffic simulation engine.

- **Enforce the processed troubleshooting action item on the live network:**

  This part comprises of a traffic simulation engine which is capable of injecting traffic to mimic any kind of application. This device could be a laptop of Aruba UXI sensor (capable of connecting to the cloud-based Aruba Central) running a specific software that can achieve the functionality of pcap replay mechanism with preloaded pcap files of various applications. Currently, traffic simulation engine is a python application that would take a pcap file and modify the IP / MAC addresses with the ones of real devices and inject the traffic to simulate bidirectional conversation to mimic any client-server application.



Traffic Simulation Engine

  The traffic simulation engine would be controlled by the AI which would determine the type of traffic to be injected into the network based on user input. The conversation would happen between two different interfaces (IF1 and IF2) with wifi interface connected wirelessly to the AP and the wired ethernet connected on the uplink side of the AP making it seem like traffic reaching the AP from an upstream device (as depicted in the figure Traffic Simulation Engine). Additionally, with a Network Interface Card (NIC) that supports virtualization, it becomes possible to simulate traffic of multiple clients which could simulate conference calls or meetings with multiple participants.

- **Analyse logs and publish results:**

  The AI would analyze the configurations, logs and stats (like tech-support logs or kernel stats) and present a dashboard containing consolidated reports that could be debugged by an expert using deeper insights and also intelligently recommend corrective actions autonomously without any manual intervention into the network (changes that can be applied to the network configurations). The AI trains itself to get better at the analysis with feedback from the user and also troubleshooting based on the suggested corrective actions taken. In addition, these troubleshooting stats could also serve as crucial feedback for AI-based intelligent network management solutions and also perform AI-driven security tests (simulating DDoS attacks or penetration tests).

Evidence the solution works

Currently, we have developed and tested a packet replay application to read a pcap file and the reliability of packet replay mechanism to address following example scenarios:

- Packet replay to simulate VoIP calls such as Teams (audio/video), Skype (audio/video), WiFi-call and observed that the UCC feature on the AP is classifying the corresponding call and obtain call quality stats which can point us to corrective actions such as setting priority to mark packets with DSCP to improve VoIP experience or modify to higher DSCP if other applications in the network are hogging more resources with DSCP marked traffic.
- If a user wants to troubleshoot reachability to a device within the network (for example a printer), the system would check which VLAN the printer device belongs to and can produce nmap host scanning results to determine any config changes are needed (like route configurations).

- CI Sanity currently performs automated sanity tests with various test beds and analyzes logs to verify functionality of various setups with the changes from the pull requests. This solution would enhance the analysis capabilities to report anomalies and suggest corrective actions in the network.

Competitive approaches

Juniper networks have developed Marvis Virtual Network Assistant based on Mist AI, which provides capabilities of intelligent network management with conversational interface. However, Marvis is only limited to troubleshooting missing VLANs, bad cables, congested WAN circuits which are event based triggers capable of detecting selective anomalies. The proposed solution enhances troubleshooting depth by reporting the actual behaviour of real traffic injected into the network, making it appear like traffic from real devices that too based on user description of the issue. Additionally, this system also provides AI-driven security testing solution with which the attack vectors can be pinpointed and eliminated from the network.

Current status

Currently, we have developed a python application to achieve packet replay functionality for the traffic simulation engine to replicate various applications such as Skype (voice and video call), Teams (voice and video call) and wifi-call and observed that the simulated traffic is successfully classified by the APs. The call quality stats are also reported by Unified Collaboration and Communication (UCC) functionality confirming that the simulated traffic was as convincing as a real call made from real devices within the network.

Next steps

The capabilities proposed by this solution could be integrated into Aruba UXI Sensors which would make them an extremely intelligent monitoring and troubleshooting devices. The solution could also be enhanced offer a custom pcap replay feature to troubleshoot network issues that are challenging to reproduce by enabling a user to upload a custom pcap. The traffic simulation engine could be enhanced to perform security tests based on pcaps to perform security attacks to troubleshoot and identify security vulnerabilities. AI-driven security testing would be a revolutionary approach to enhance the precision of security tests and seamlessly adapting to newer threats that emerge.

References

Marvis Virtual Network Assistant

Cisco AI Assistant