Technical Disclosure Commons

Defensive Publications Series

December 2019

OUTCOME OF MACHINE REASONING IN A NETWORK MANAGEMENT SYSTEM TOPOLOGY VIEW

Michael Michaelides

Arabinda Samantaray

Ajay Madhavan

Samer Salam

Smruti Lele

See next page for additional authors

Inventor(s)
Michael Michaelides, Arabinda Samantaray, Ajay Madhavan, Samer Salam, Smruti Lele, and Ashwini Manerikar

OUTCOME OF MACHINE REASONING IN A NETWORK MANAGEMENT SYSTEM TOPOLOGY VIEW

AUTHORS:
Michael Michaelides
Arabinda Samantaray
Ajay Madhavan
Samer Salam
Smruti Lele
Ashwini Manerikar

ABSTRACT

A technique is described herein to provide a visualization overlaid on a network topology that illustrates the cascading impact of a network event before it happens. The technique may empower a network administrator to perform one or more steps to mitigate the issue and/or minimize its impact before the issue manifests itself into a critical network condition.

DETAILED DESCRIPTION

On any normal day, even if a network is functioning correctly, this does not imply that there are no underlying issues or sub-optimal configurations that might negatively impact the performance of the network. Subtle changes in the network, such as a Media Access Control (MAC) address flap or a Central Processing Unit (CPU) spike, might be expected as users roam through Access Points or an elephant flow is happening, or they might also be indicative of a potentially serious issue. In the absence of a succinct topology view that correlates such subtle indicators with the catastrophic impact that they could cause, if left unchecked, a network administrator (admin) could easily ignore such indicators.

This proposal provides a technique for enabling network administrators to visualize, ahead of time, the potential impact of disruptive failures such as, for example, Spanning Tree Protocol (STP) loops, etc. on clients and services running in a network. By monitoring changes in network environment, the technique may provide for performing rule-based analysis to determine if any significant disruption or change in the network is likely to happen based on machine-reasoning outcomes. Conclusions derived from such machine-

reasoning could be illustrated on the network topology to provide a network admin with insight into the nature of potential disruption(s), severity of such disruption(s), and subsequent impact(s) on the network. A novelty of this technique may include providing a visualization, overlaid on the network topology, of the cascading impact of a network event beforehand, which may empower a network admin to take one or more steps to mitigate the issue or minimize its impact before it manifests itself into a critical network condition.

The technique may provide various capabilities including, but not limited to: filtering out irrelevant parts of a network to allow a network admin to focus on an impacted area; providing visualizations of directly impacted devices and explanations of the possible occurring issue; providing evaluations regarding whether the network may still be functional or not functional after the issue, and provide explanations for either scenario, in the enhanced topology view; providing visualizations of subsequent events in phases, which can happen in case the predicted event manifests, and how each of these may impact the devices and links in the network; and for each subsequent event that may occur in the network on the manifestation of the issue, the technique may provide customized recommendations so that the network admin can take appropriate steps to minimize the impact.

Consider an example scenario in which there is a fan failure on a power supply that is leading to an increase in device temperature above a recommended threshold on a device labeled 'DEVICE11', as shown in Figure 1, below.

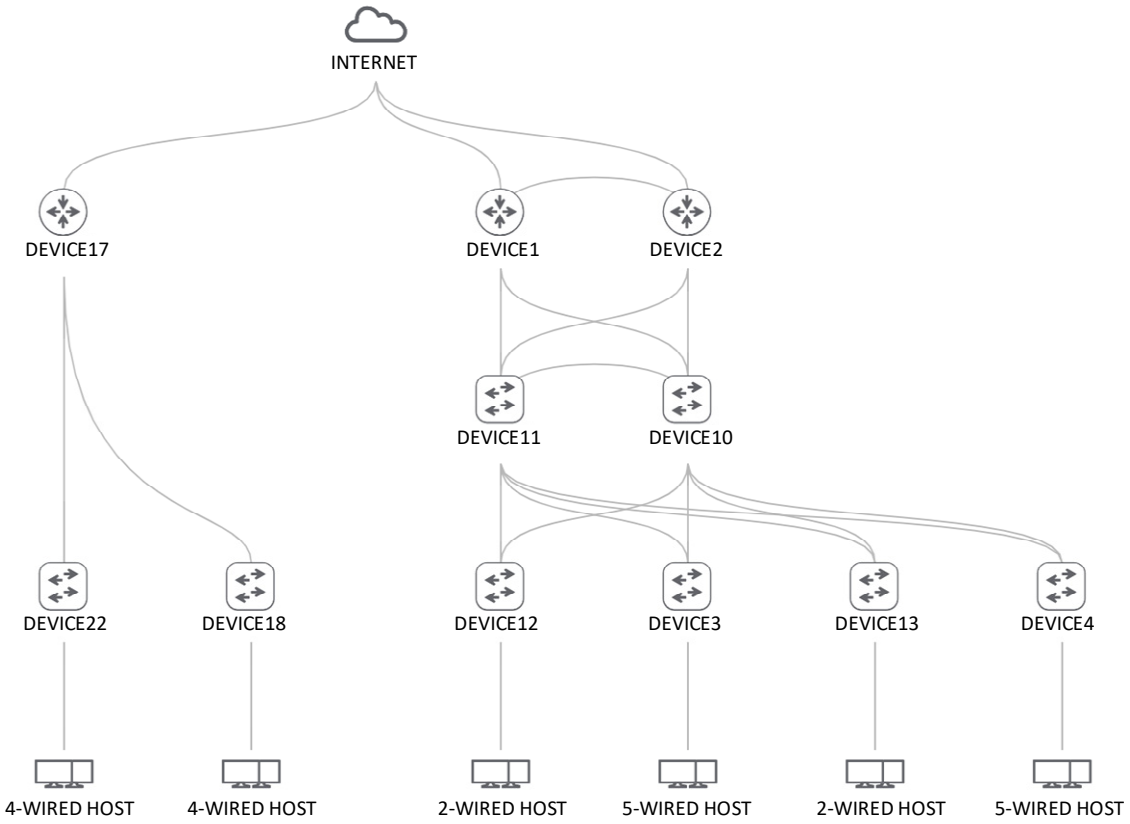

Figure 1

According to the technique proposed herein, the presence of such an abnormal network condition can trigger a Semantic Reasoner to identify that DEVICE11 is in risk of suffering a power supply unit (PSU) failure. In the subsequent step, the Semantic Reasoner collects additional information and identifies the following factors that will influence the impact of this issue such as, but not limited to: a role of the device (e.g., access, distribution, etc.); services provided to the network by the device (e.g., default gateway, Dynamic Host Configuration Protocol (DHCP) server, etc.); Layer 2 (L2) information, which may include centrality/importance of the device in a spanning tree (e.g., a root bridge failure will cause temporary STP recalculation, which can cause a disruption); data flow information for load balancing (e.g., if the node is part of a load balancing group); and/or whether any redundancy may be available in the network (e.g. will the network be able to re-converge in the case of failure of this device).

In the illustrated example, consider that DEVICE11 is a distribution switch, the spanning tree root bridge for certain virtual local area networks (VLANs), and part of a load balancing group. Thus, for the present example, an enhanced topology view may be

displayed, as shown in Figure 2, below, in which the unaffected portion of the network is removed from the view and the concerned device is highlighted as vulnerable to a PSU failure. Additionally, the above important factors are displayed as critical information that can be used for impact analysis decisions.

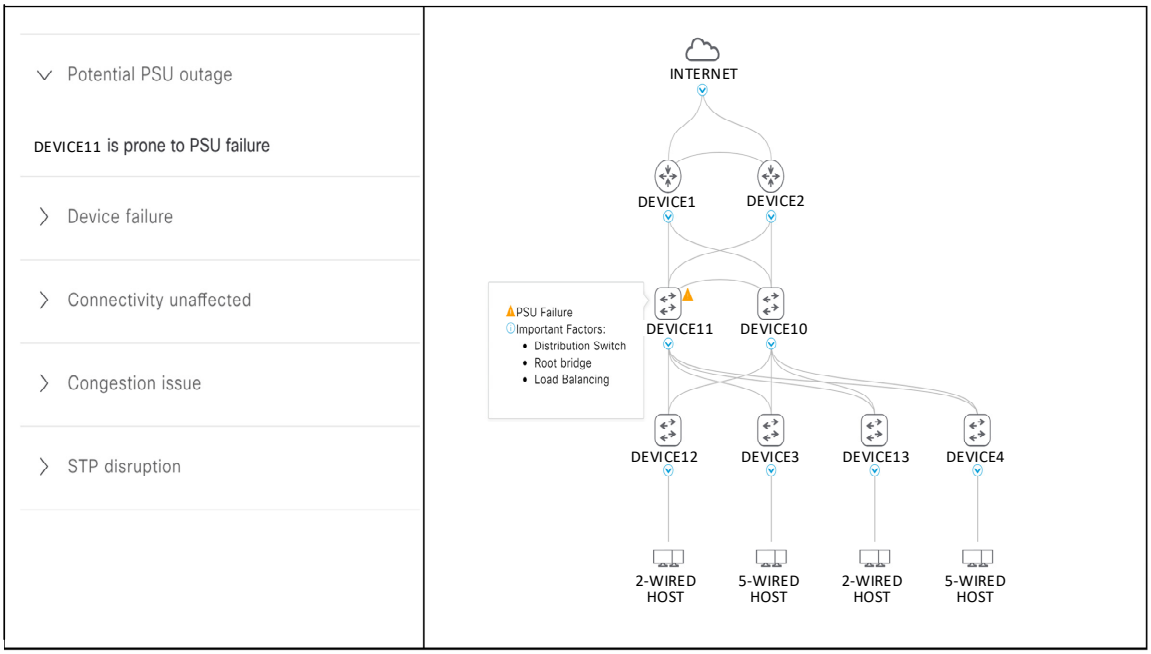

Figure 2

Based on the earlier derived conclusion, direct impact to the network can be illustrated. For the present example, DEVICE11 is in risk of suffering a PSU failure. Thus, eliminating it and its associated links from the active topology can be viewed as shown in Figure 3, below, by highlighting DEVICE11 along with its links in red.

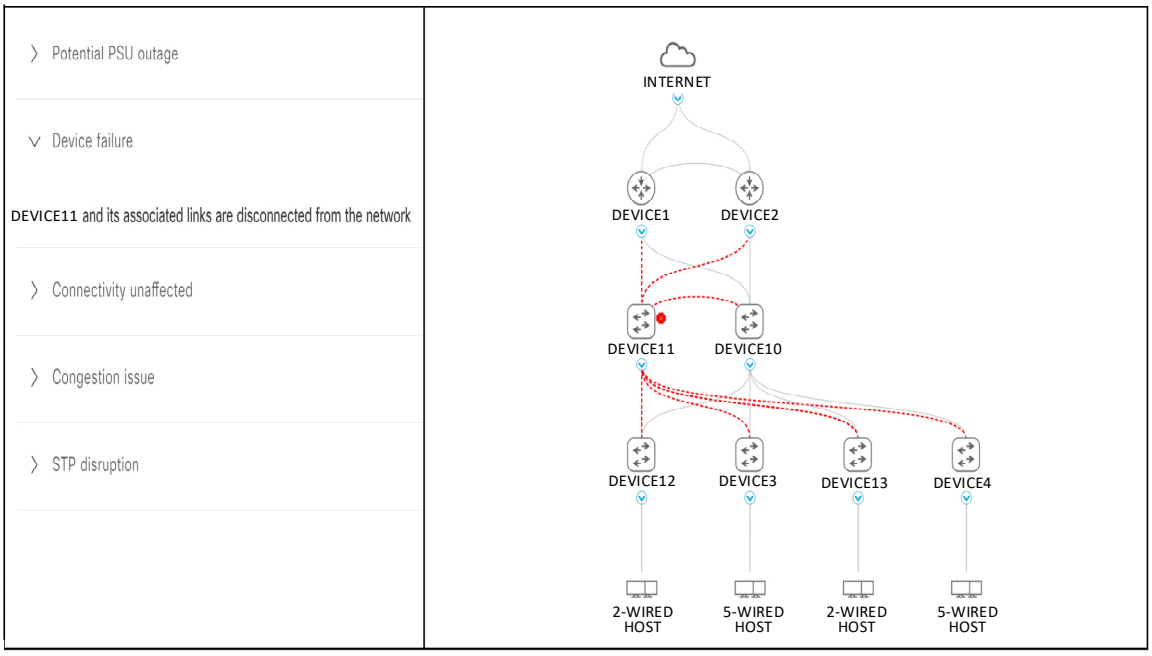

Figure 3

The resulting topology can be evaluated to determine whether full connectivity exists or not after the occurrence of the issue. If full connectivity does not exist then parts of the network have lost connectivity can be displayed. This can be illustrated by comparing Figures 4(a) and 4(b), as shown below.

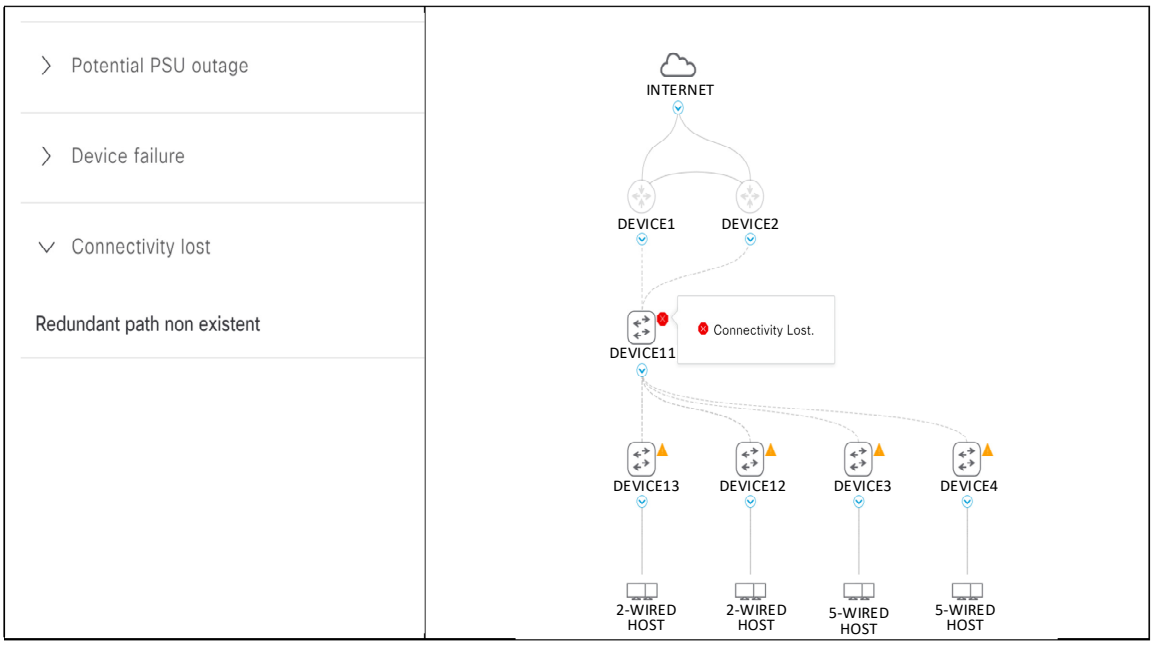

Figure 4(a)

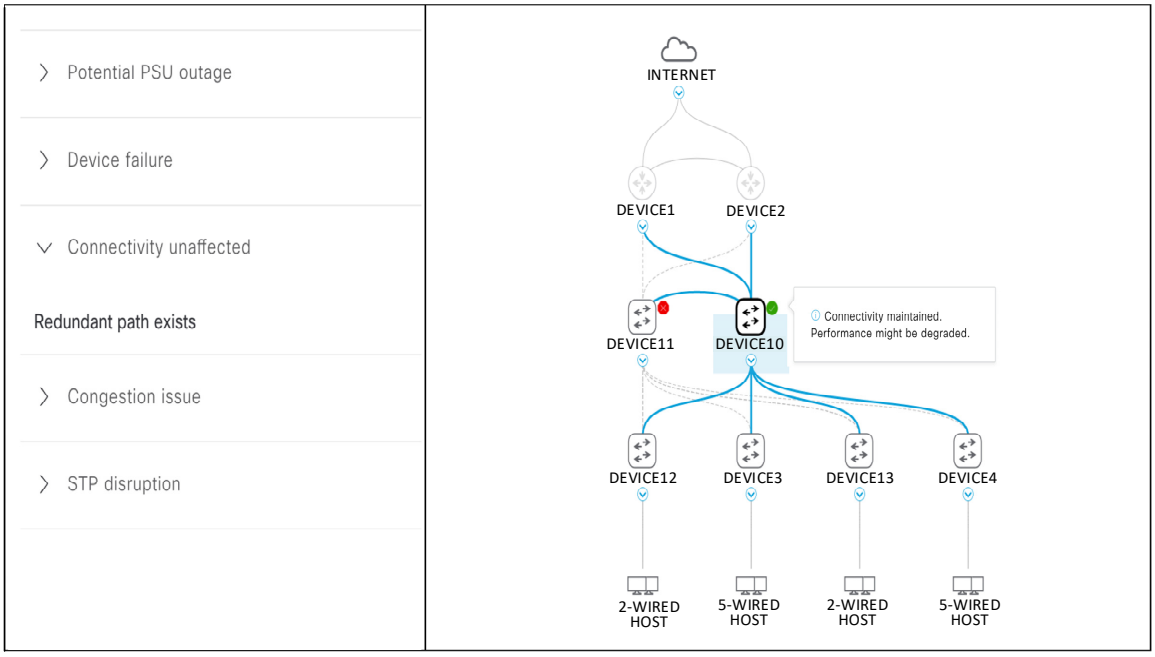

Figure 4(b)

In Figure 4(a), where there is no alternative path to the distribution layer, the access layer device and the hosts on them are highlighted as disconnected from the network along with an appropriate message indicating the high severity of the issue. In Figure 4(b), where there is an alternative path due to the presence of DEVICE10, connectivity is still maintained as indicated by the corresponding message.

For cases in which connectivity may be maintained, the possibility of performance degradation can be evaluated and displayed as a series of progressive events that can, for example, be displayed on the panel in the left-hand side. Each panel event can be selected to get a more detailed visualization of the issue on the enhanced topology view.

In the illustrated example, DEVICE11's PSU failure may cause two events including decreased load balancing and STP root elections and tree re-calculation that may be identified by the Semantic Reasoner based on factors discussed above.

Consider decreased load balancing, for example. Since the access switches (DEVICE12/3/13/4) now have only one uplink remaining then load balancing between VLAN traffic is eliminated, which can lead to congestion on the uplink, thereby affecting the performance of the network and the experience of the users. This is indicated by

highlighting the congested uplink as well as the affected devices and hosts as shown in Figure 5, below.

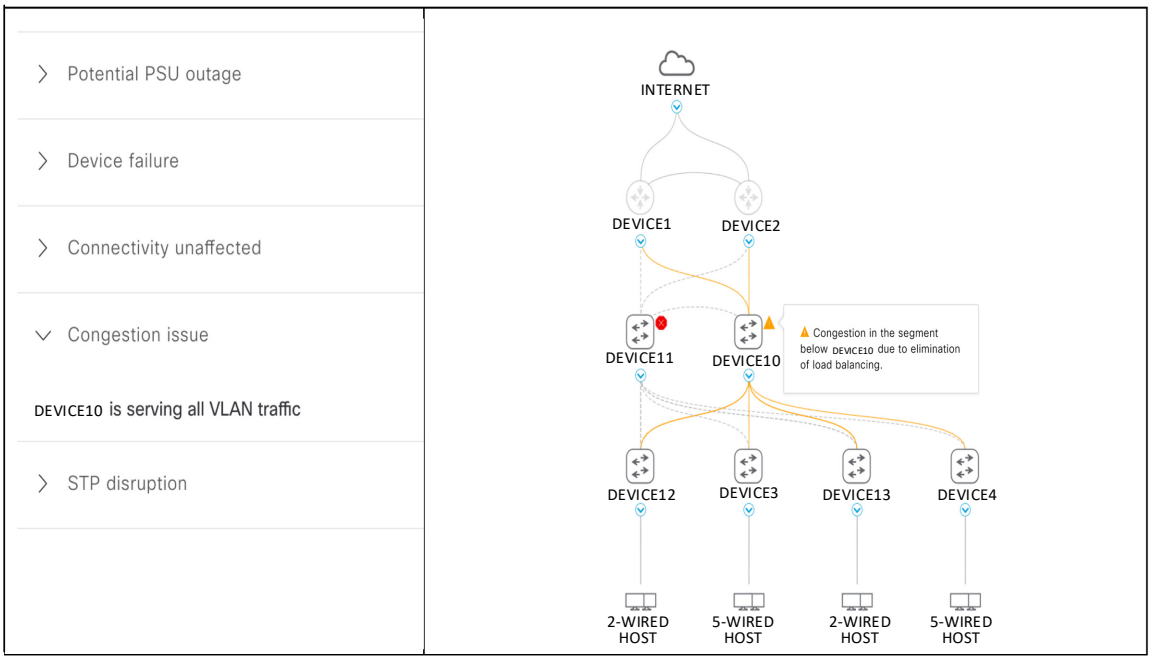

Figure 5

Additionally, the spanning tree may need to be recalculated for the VLANs where DEVICE11 is the root bridge, which may cause a temporary disruption. Under an assumption that DEVICE4 takes over as the new root bridge, then the logical topology of these VLANs may change (e.g., ports currently forwarding might start blocking and vice versa). Additionally, since the new root bridge is an access switch, then the resulting topology may be suboptimal. This is illustrated in Figure 6 in which the new root bridge and the new forwarding links are highlighted along with a notification for the temporary disruption and the suboptimal topology.

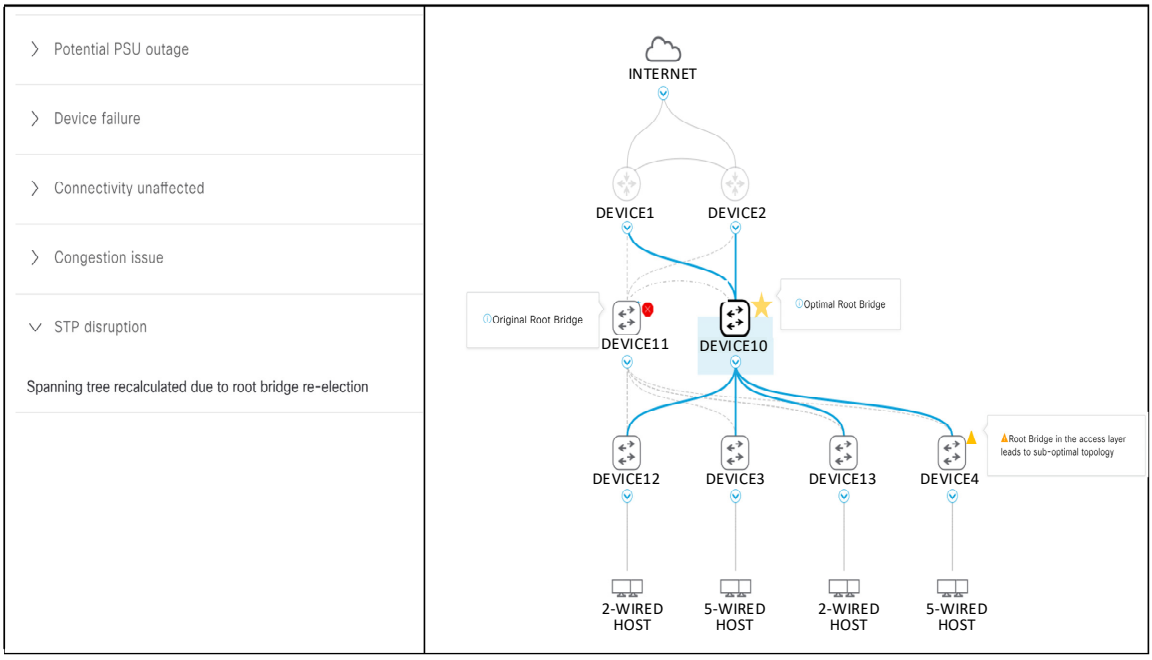

Figure 6

Accordingly, automated prediction of possible issues in a network based on environmental conditions of the network may be facilitated by the interplay among various components and/or supporting backend information including, but not limited to, data collectors, the Semantic Reasoner, topology data, and an enhanced topology view of the network.

The Semantic Reasoner may be a machine reasoning framework, which may operate on a network management system in order to provide for the ability to automate network troubleshooting. In some instances, the Semantic Reasoner may operate on domain knowledge that may be defined in a formal semantic model (ontology) using Web Ontology Language (OWL) and Semantic Web Rule Language (SWRL).

There may be two different types of data collectors including listeners and device pollers. Listeners, such as Simple Network Management Protocol (SNMP) traps and/or Syslog collectors, may constantly or periodically provide the Semantic Reasoner with data and/or information relating to any changes in the network environment, which may automatically trigger reasoning by the Semantic Reasoner. Device pollers may be responsible for polling devices in the network and collecting real-time data from the devices for further analysis. In some instances, topology data may be provided by a

network management system and may enable the Semantic Reasoner to understand the topology of the network and details about the devices.

As discussed above, current topology views are limited to showcasing nodes, links, and their respective health scores. In contrast, the topology view of the proposed technique can provide new visualizations not just for the root cause of possible network issues but also their spreading impact on the network. In addition, appropriate recommendations to negate the impact of such issues can greatly enhance a user's experience.

In summary, the novelty of the technique described herein is to provide a visualization overlaid on a network topology that illustrates the cascading impact of a network event before it happens. Thus, a network administrator may be empowered to perform one or more steps to mitigate the issue and/or minimize its impact before the issue manifests itself into a critical network condition.