April 2020

SOFTWARE TO AUTOMATE WIFI NETWORK DEPLOYMENTS

N/A

SOFTWARE TO AUTOMATE WIFI NETWORK DEPLOYMENTS

ABSTRACT:

The technology relates to a vendor-neutral frontend for configuring and monitoring mobility solutions. Through the vendor-neutral frontend, a heatmap for a premise may be used/optimized, which may include a plurality of access points at various locations on the premise. Hardware-specific information on the mobility access points to be deployed may also be gathered through the vendor-neutral frontend. Based on the heatmap and the hardware-specific information, vendor-neutral configurations may be generated, and pushed to the mobility access points to create an operating network. Once the network is operational, the frontend may be used to monitor telemetry data from the mobility access points, which may be used as feedback to update the heatmap.

BACKGROUND:

Enterprise IT teams struggle with lack of multivendor mobility solutions that can be deployed and managed with a single control interface. Vendors of mobility equipment, such as WiFi access points, provide vendor-specific assistance with configuration and/or monitoring for their own equipment. Different vendors have different ways of configuring and monitoring their own equipment, which may include different protocols, control interfaces, etc. As such, most enterprises choose to deploy vendor proprietary solutions for their mobility needs with an all or nothing approach. These single vendor solutions, which are most often based on proprietary technology, thus prevent enterprises from having freedom-of-choice in their vendor-selection, which propagates vendor lock-in and stifling innovation. Further, within a single vendor solution, deployment of the wireless network may take a long time due to the lack of automation capabilities for initial setup and configuration, as well as for monitoring ongoing operations.

DETAILS:

The technology relates to a vendor-neutral frontend for configuring and monitoring mobility solutions from multiple vendors. Through the vendor-neutral frontend, a heatmap for a premise may be used/updated, which may include a plurality of locations where access points are to be placed. Hardware-specific information on the mobility equipment to be deployed may also be gathered through the vendor-neutral frontend. Based on the heatmap and the hardware-specific information, vendor-neutral configuration may be generated by the frontend, and pushed to the mobility access points to create an operating network. Once the network is operational, the frontend may be used to monitor telemetry data received from the mobility access points, which may be analyzed and used as feedback to update the heatmap and/or configurations of the mobility access points.

FIGURE 1 below provides an example workflow using the frontend. The frontend may be implemented as a software, which may be run on one or more processors.

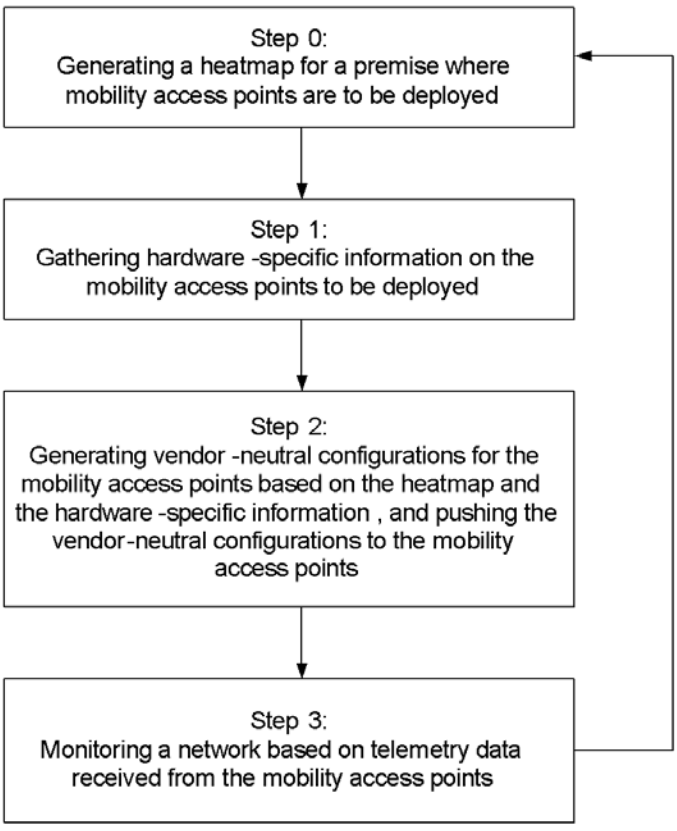

FIGURE 1

Referring to FIGURE 1, at Step 0, a heatmap may be generated for a premise where mobility access points are to be deployed. For example, the premise may be an office building with multiple rooms and/or floors, or an apartment complex with multiple buildings. The mobility access points may be from multiple vendors, who may use different configuration protocols and interfaces. The heatmap may be generated as any graphical representation, such as a picture or a CADmap. For instance, a floorplan of the premise may be uploaded to the frontend as an image. The heatmap may indicate expected signal strengths at various locations of the premise based on planned locations of access points on the premise. For instance, planned locations for a predetermined number of mobility access points may be received as input from a user, such as a network operator planning the deployment. By way of example, the user may provide the floorplan and planned locations for access points to a web-based application, such as a web-based slides application. A heatmap of expected signal strengths may then be generated on the floorplan of the premise based on the input. In this regard, the heatmap may be accessible using the frontend through an application programming interface (API). For example, planned locations for access points may be received by the frontend, through an API, from the web-based application.

The heatmap generated may be outputted on a display, such as a monitor or a screen, for viewing by the user. The user may then install the mobility access points at the locations according to the heatmap. In some instances, the user may make adjustments to the planned locations of the mobility access points. For example, if the heatmap shows that certain locations of the premise would have weak or no signal coverage with the current planned locations of the mobility access points, the user may adjust the locations of the mobility access points on the floorplan of the premise, and/or add more mobility access points. The frontend may then update the heatmap according to the adjustments.

At Step 1, hardware-specific information on the mobility access points to be deployed may be gathered. For example, the equipment to be deployed may be WiFi access points from multiple vendors. Hardware-specific information on the equipment may be gathered by scanning barcodes on the mobility access points using a scanner on a mobile or portable device. In this regard, the hardware-specific information may include MAC addresses of the mobility access points, brand and model of the mobility access points, etc. The gathered information may be stored using a web-based application, such as a web-based spreadsheet application, through an API. For example, the device being used for scanning the mobility access points may also run an instance of the web-based spreadsheet, such that, as the information is being scanned, the information may be provided to the web-based spreadsheet through the API. As such, the various access points and the respective hardware-specific information may be stored as entries on a spreadsheet. The web-based application may make the stored hardware-specific information accessible to the frontend, for example also through an API. As such, the user may view the entries on the spreadsheet through the frontend.

At Step 2, vendor-neutral configurations may be generated for the mobility access points based on the heatmap and the hardware-specific information, and the vendor-neutral configurations may be pushed to the mobility access points. In this regard, the frontend may use language bindings to generate vendor-neutral configurations based on the heatmap and the hardware-specific information collected. The configurations may include naming for the mobility access points, configuration of radio properties, such as channels, channel width, transmit power, as well as configuration of network names and network security options. In this regard, the frontend may provide the user access to the heatmap and the hardware-specific information, and the configuration options. The operator may select among the options and/or make adjustments to default configurations through the frontend. The frontend may then push

the vendor-neutral configurations to the mobility access points. Once the mobility access points are configured according to the vendor-neutral configurations, the network is operational.

At Step 3, during operation, the network may be monitored based on telemetry data received from the deployed mobility access points. For instance, the frontend may provide access of the telemetry data, and/or analytics of the telemetry data to the user. Based on the analytics, issues with the network may be identified. As an example, the telemetry data may indicate that current placements of the mobility access points provide weak or no signal coverage at certain areas within the premise. As another example, the telemetry data may indicate that the current channel configurations create load imbalance or congestion. Thus, results of this analysis may be used as feedback to Step 0, where locations of the mobility access points may be adjusted accordingly. Additionally or alternatively, the results of the analysis may also be used as feedback to Step 2, where aspects of channel planning may be adjusted accordingly.

FIGURE 2 shows an example system for configuring and monitoring WiFi access points from multiple vendors. As shown, the system includes components for configuring and deploying mobility access points, as well as components for monitoring operations of the mobility access points. The frontend, which is shown as “Config Generator,” is in communication with a web-based slides application shown as “gSlides,” and with a web-based application shown as “gSheet.” As described above, the Config Generator may provide users access to heatmaps of premises through gSlides. For instance, the Config Generator may use the heatmaps as one of the sources of truth, and may update the heatmaps based on telemetry data. The Config Generator may also provide users access for gathering hardware-specific information on the equipment to be deployed through gSheet. For example as shown, hostname

and MAC may be provided to the Config Generator. In this regard, gSheet may be provided with access to an application on a device that gathers the hardware-specific information, shown as "Provisioning App."

The Config Generator may generate vendor-neutral configurations based on a heatmap. The Config Generator may generate vendor-neutral configurations using "OpenConfig Language Bindings. Once the vendor-neutral configurations are generated, Config Generator may push the vendor-neutral configurations to the mobility access points. As mentioned above, the configurations may include naming of the mobility access points, channel planning, etc., and may be pushed to the mobility access points according to an OpenConfig protocol shown as "gNMI." The configuration generator may also update network related systems such as the network's IP Address Management (IPAM) according to protocols such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS).

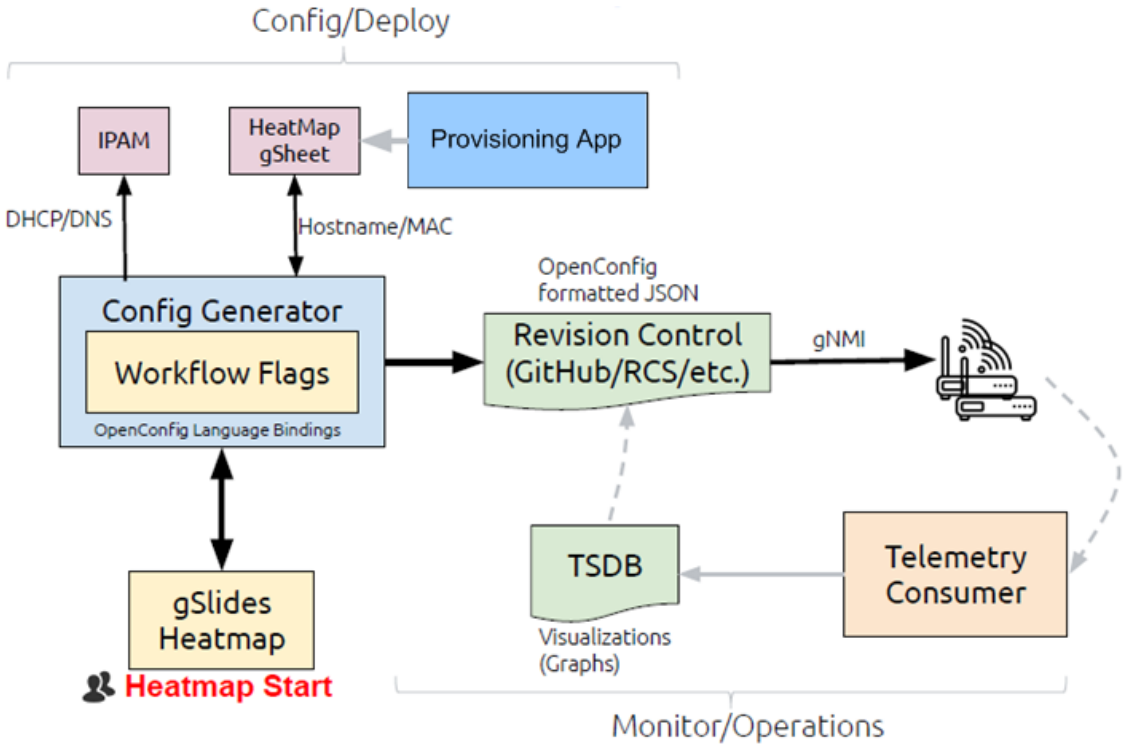

FIGURE 2

Further as shown, during operation of the network, telemetry data may be received from the deployed mobility access points. The telemetry data may be collected in a database, such as a Time Series Database (TSDB). Analytics may be generated based on the telemetry data, under which issues with the current network configuration may be identified. In some instances, visual representation such as graphs may be generated based on the telemetry data. Based on the analytics, adjustments may be made to the vendor-neutral configurations generated by the Config Generator, and stored in the "Revision Control System" as shown. Additionally or alternatively, adjustments may be made to the heatmap, for example by adding, removing, or changing location of the mobility access points.

The technology is advantageous because it provides a vendor-neutral frontend for configuring and monitoring mobility access points. The vendor-neutral frontend provides enterprise IT teams a centralized, automated, and user-friendly interface for configuring and monitoring mobility access points from multiple vendors. Features of the technology further provides for monitoring of the network during operation, which may be used to improve coverage and channel planning. In addition, with the vendor-neutral frontend, enterprise IT teams may select access points from different vendors with different features that meet specific needs of the enterprise. The flexibility thus prevents vendor lock-in and promotes innovation.