November 16, 2018

IDENTIFYING ACCESS POINTS ON THE PHYSICAL PERIPHERY OF A DEPLOYMENT

Sajjit Thampy

Zach Cherian

IDENTIFYING ACCESS POINTS ON THE PHYSICAL PERIPHERY OF A DEPLOYMENT

AUTHORS:
Sajjit Thampy
Zach Cherian

ABSTRACT

Techniques are provided for eliminating noisy alerts and bringing more relevant actionable alerts to the attention of a wireless network operator in an intent based system. This may be accomplished by differentiating and determining Access Points (APs) on the network periphery and down-weighting certain classes of problems.

DETAILED DESCRIPTION

Access Points (APs) may be deployed as part of wireless solutions to commercial locations such as big box retail stores, hospitals, airports, etc. When users walk into these establishments, their devices typically connect to the nearest AP. This collective activity causes a lot of alert-clutter on a network operator's alerts dashboard.

Techniques are described to automatically identify APs that are on the physical periphery of a network. This knowledge of peripheral APs may be used to provide an appropriate relevance level for associated alerts. For example, a network infrastructure may indicate poor Radio Frequency (RF) for a client approaching the establishment or that a client is initially unable to on-board. These indication may be suppressed or lowered based on an attention/relevance scale. This enables the management system to avoid cluttering monitoring dashboards with irrelevant issues and focus on providing a good wireless experience internal to the premises. This makes the network infrastructure more intent based.

Alerts may be triggered by a network infrastructure based on data from wireless APs in the establishment. The client devices may be wireless devices such as smart phones, smart watches, etc. The network operator has dashboards that show devices that are experiencing RF issues, interference, on-boarding issues, and faulty APs. Often, network APs on the periphery of a deployment tend to surface more frequently on these dashboards because clients are in parking lots, walking into the establishment, etc.

Published by Technical Disclosure Commons, 2018

Figures 1 and 2 below illustrate an example of alert-clutter that tends to occur in a network infrastructure solution. As shown, the topmost alerts actually occur but are not relevant to the network operator. For example, these may result from client devices operating in the periphery of the deployment (e.g., clients in parking lots, moving towards or away from doors, standing near/outside buildings, etc.).

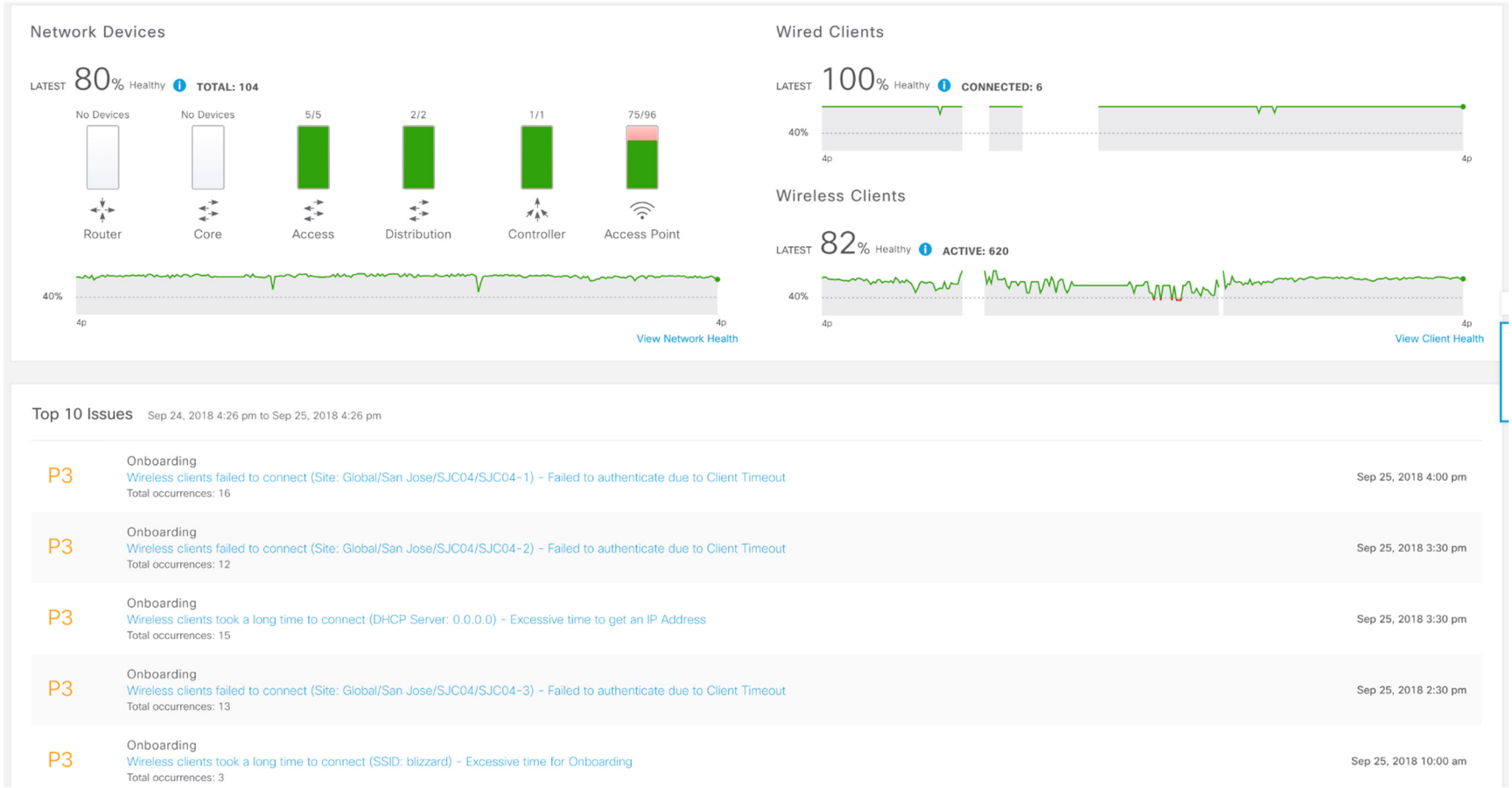
Network Devices
LATEST 80% Healthy
TOTAL: 104
No Devices
No Devices
5/5
2/2
1/1
75/96
Router
Core
Access
Distribution
Controller
Access Point
40%
4p
4p
View Network Health
Wired Clients
LATEST 100% Healthy
CONNECTED: 6
40%
4p
4p
Wireless Clients
LATEST 82% Healthy
ACTIVE: 620
40%
4p
4p
View Client Health
Top 10 Issues
Sep 24, 2018 4:26 pm to Sep 25, 2018 4:26 pm
P3
Onboarding
Wireless clients failed to connect (Site: Global/San Jose/SJC04/SJC04-1) - Failed to authenticate due to Client Timeout
Total occurrences: 16
Sep 25, 2018 4:00 pm
P3
Onboarding
Wireless clients failed to connect (Site: Global/San Jose/SJC04/SJC04-2) - Failed to authenticate due to Client Timeout
Total occurrences: 12
Sep 25, 2018 3:30 pm
P3
Onboarding
Wireless clients took a long time to connect (DHCP Server: 0.0.0.0) - Excessive time to get an IP Address
Total occurrences: 15
Sep 25, 2018 3:30 pm
P3
Onboarding
Wireless clients failed to connect (Site: Global/San Jose/SJC04/SJC04-3) - Failed to authenticate due to Client Timeout
Total occurrences: 13
Sep 25, 2018 2:30 pm
P3
Onboarding
Wireless clients took a long time to connect (SSID: blizzard) - Excessive time for Onboarding
Total occurrences: 3
Sep 25, 2018 10:00 am

Figure 1

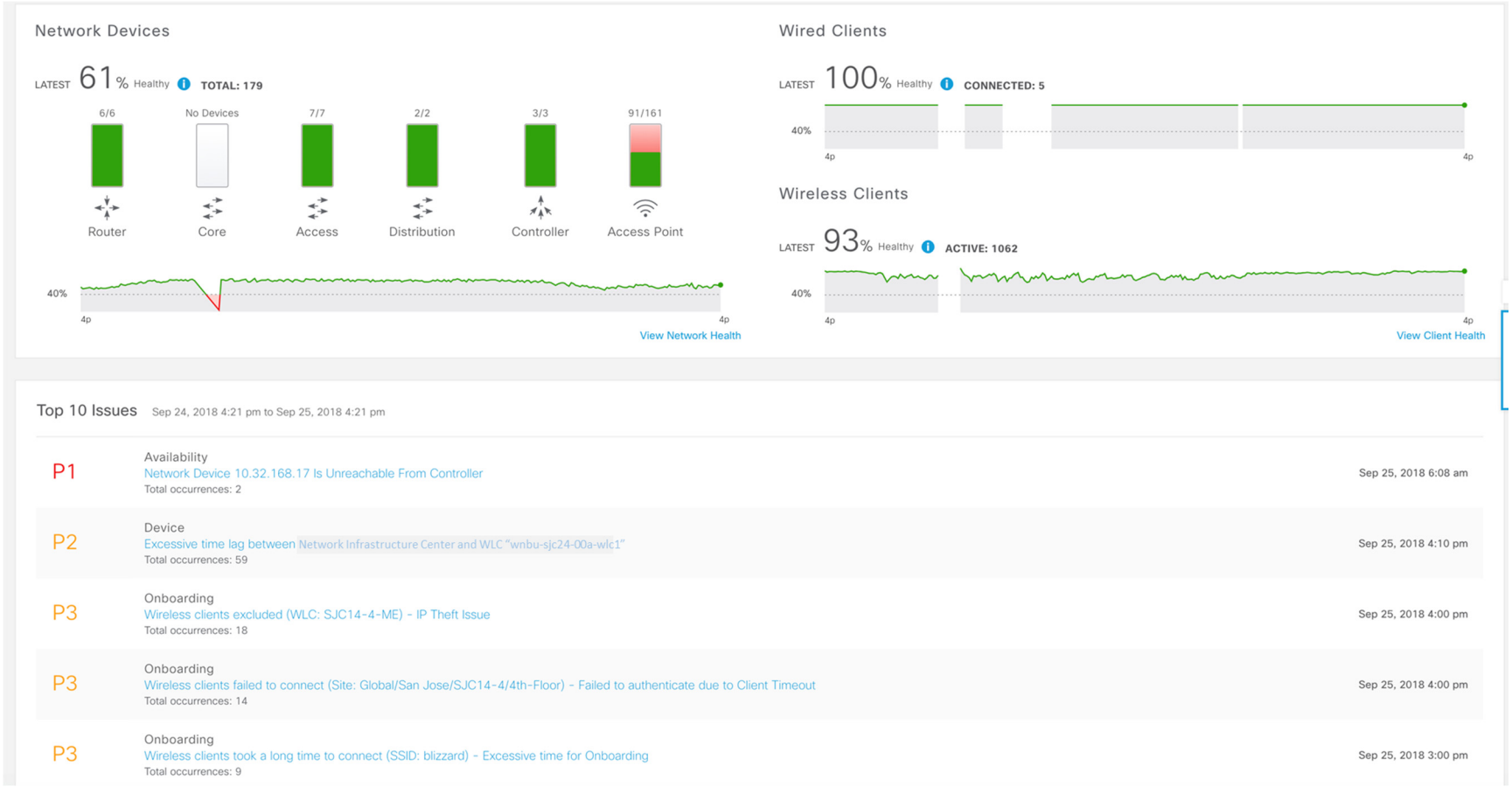
Network Devices
LATEST 61% Healthy
TOTAL: 179
6/6
No Devices
7/7
2/2
3/3
91/161
Router
Core
Access
Distribution
Controller
Access Point
40%
4p
4p
View Network Health
Wired Clients
LATEST 100% Healthy
CONNECTED: 5
40%
4p
4p
Wireless Clients
LATEST 93% Healthy
ACTIVE: 1062
40%
4p
4p
View Client Health
Top 10 Issues
Sep 24, 2018 4:21 pm to Sep 25, 2018 4:21 pm
P1
Availability
Network Device 10.32.168.17 Is Unreachable From Controller
Total occurrences: 2
Sep 25, 2018 6:08 am
P2
Device
Excessive time lag between Network Infrastructure Center and WLC "wnbu-sjc24-00a-wlc1"
Total occurrences: 59
Sep 25, 2018 4:10 pm
P3
Onboarding
Wireless clients excluded (WLC: SJC14-4-ME) - IP Theft Issue
Total occurrences: 18
Sep 25, 2018 4:00 pm
P3
Onboarding
Wireless clients failed to connect (Site: Global/San Jose/SJC14-4/4th-Floor) - Failed to authenticate due to Client Timeout
Total occurrences: 14
Sep 25, 2018 4:00 pm
P3
Onboarding
Wireless clients took a long time to connect (SSID: blizzard) - Excessive time for Onboarding
Total occurrences: 9
Sep 25, 2018 3:00 pm

Figure 2

The algorithm proceeds in the following steps once data is collected from the network infrastructure. It is determined which clients (denoted by Media Access Control (MAC) addresses) are associated with which AP. The associations may be timestamped.

At a first example step, all the associations of a client MAC address with various APs are time-sorted. The data set below may be collected by the network infrastructure and may represent clients accessing APs that join a network for a given day.

AP1, 11:00am, iPhone®-client-A

AP1, 11:00am, Android™-client-C

AP1, 11:01am, iPhone-client-B

AP2, 11:03am, iPhone-client-A

AP2, 11:05am, Android-client-C

This may be transformed into

iPhone-client-A, AP1, AP2

iPhone-client-B, AP1

Android-client-C, AP1, AP2

At a second example step, a rank order metric is computed for every AP in the transformed dataset. The rank order metric seeks to estimate the likelihood that a given AP is on the periphery. This may be estimated using the network infrastructure cloud or an on-premise agent for a given client.

$$Likelihood(AP|Rank = i, Client) = \frac{Rank_i}{max\{Rank_i\}}$$

This process may be repeated for all clients and an average taken for each AP.

$$Likelihood(AP|Rank = i) = \frac{1}{N_{clients}} \sum_{Clients} \frac{Rank_i}{max\{Rank_i\}}$$

As an example, for each AP, its relative normalized rank order may be computed. In the example above, the relative rank order for AP1 may be 1/2 = 0.5 based on iPhone-client-A and 1/1 = 1.0 based on iPhone-client-B. Thus its overall rank order may be (1 + 0.5)/2 = 0.75.

Following the same process for AP2, 2/2 = 1.0 for iPhone-client-A and 2/2 = 1.0 for Android-client-C. Thus, its overall rank order may be (1 + 1)/2 = 1.0. The process yields

[AP1 (0.75), AP2(1.0)] as likelihood estimates for the APs being on the periphery of a deployment.

Having discovered this, to use truly intent based networking, the system down-weights all alerts that come in from AP1 by a factor shown in the likelihood score. The network health metrics, when displayed on a dashboard, are likely to have more relevant actionable insights because of the discovered physical topological significance of the APs. The down-weighting also leads to natural up-weighting of faults that happen to a non-peripheral AP within a deployment. This in turn causes improved ranking of alerts.

Figure 3 below illustrates an example environment in which the techniques described herein may be deployed.

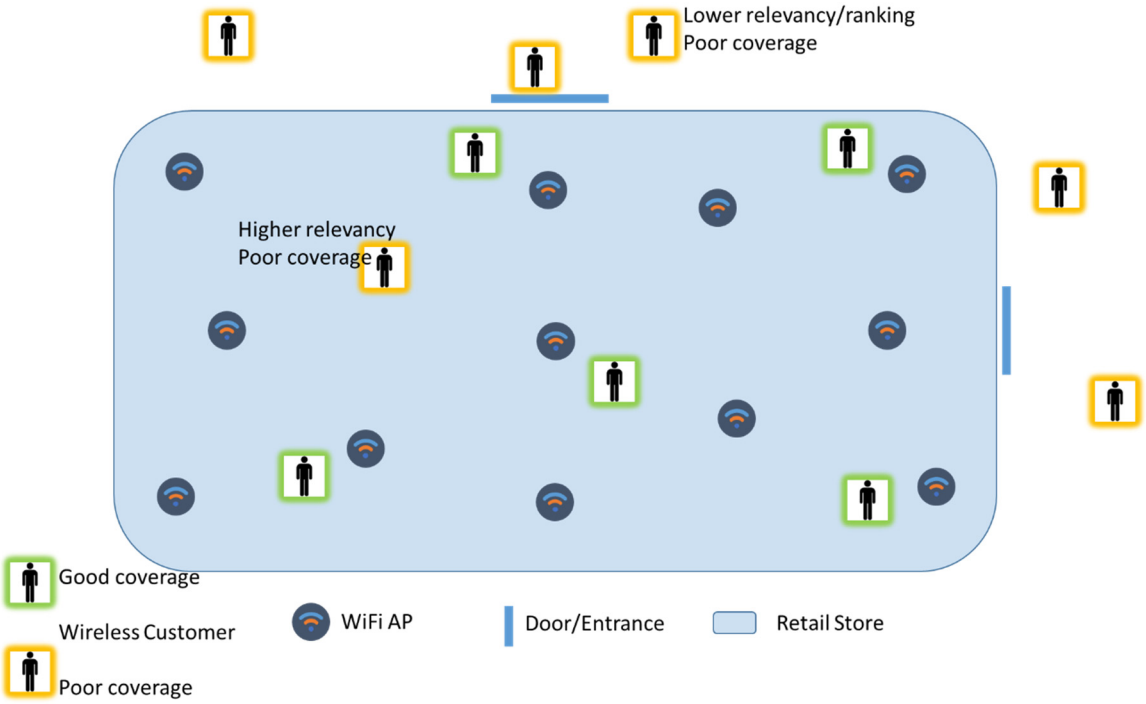

Figure 3

In summary, techniques are provided for eliminating noisy alerts and bringing more relevant actionable alerts to the attention of a wireless network operator in an intent based system. This may be accomplished by differentiating and determining APs on the network periphery and down-weighting certain classes of problems.