Technical Disclosure Commons

Defensive Publications Series

May 2020

# Rapid Integration Of WiFi Hotspots With A Cloud-based AAA Service

Huaiyu Liu

Timothy D. R. Hartley

# Rapid Integration Of WiFi Hotspots With A Cloud-based AAA Service

ABSTRACT

Public WiFi is typically provided by a network of smaller (local-area), independent service providers internetworked by a larger (wide-area) service provider. Currently, integration between the local-area and the wide-area service providers is a tedious process. This disclosure describes a set of vendor-agnostic application program interfaces (APIs) that enable a WiFi hotspot provider to integrate its control plane with a cloud-based authentication, authorization, and accounting (AAA) service in a self-service manner, without the direct involvement of personnel from the cloud service. This set of APIs enable a WiFi provider to self-register and self-configure its WiFi devices, such as controllers, with the cloud-based AAA service. Once registered and configured, the WiFi device can send requests to the cloud-based AAA service for creating WiFi sessions to control and account for users' network access.

KEYWORDS

- Public WiFi
- Captive portal
- Authentication, authorization, accounting (AAA)
- Credential provisioning
- WiFi hotspot
- WiFi control plane
- Cloud-based AAA
- WiFi provider
- Hotspot provider

## BACKGROUND

Public WiFi is typically provided by a network of smaller (local-area), independent service providers internetworked by a larger (wide-area) service provider. The local-area service providers or entities set up access points (AP) in the field, while the larger service provider or entity provides back-end support. One service provided by the wide-area entity is authentication, authorization, and accounting (AAA). Authentication serves to verify the identity of a user that seeks WiFi coverage; authorization enables a user to access network services; and the accounting service measures the time and resources used by the user, e.g., to generate an invoice.

Currently, integration between the local-area and the wide-area service providers is a tedious process. For example, registration and configuration of WiFi hotspots is a time-consuming, vendor-specific exercise. Each vendor has its own onboarding flow, and integrating with vendors to enable a managed WiFi hotspot system often entails custom work for each vendor. There are smaller service providers and venues that are interested in WiFi monetization, but the complexity of onboarding with the back-end platform prevents them from signing up. Effectively, only local-area WiFi service providers with a certain minimum size or access to resources can cost-effectively integrate with the back-end provider to provide public WiFi.

## DESCRIPTION

This disclosure describes a set of general, vendor-agnostic, application program interfaces (APIs) that enable a WiFi hotspot provider to integrate its control plane with a cloud-based AAA service in a self-service manner, without the direct involvement of personnel from the cloud service. This set of APIs enable a WiFi provider to self-register and self-configure its WiFi devices, such as controllers, with the cloud-based AAA service. Once registered and

configured, a WiFi device can send requests to the cloud-based AAA service for creating WiFi sessions to control and account for users' network access.

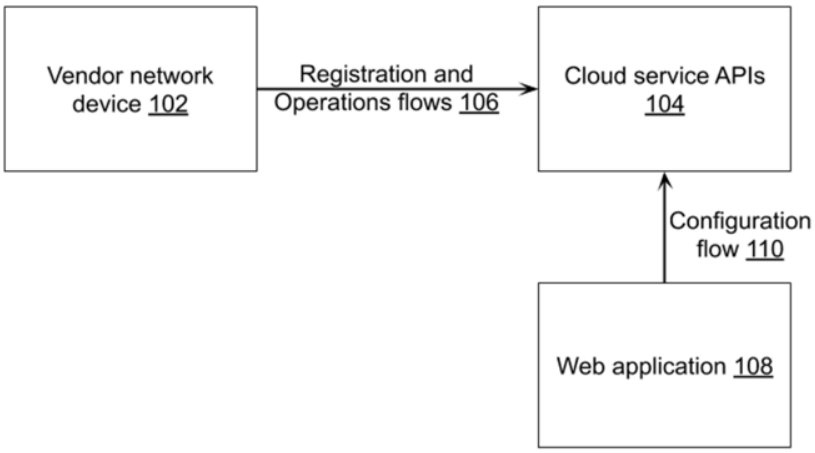


**Fig. 1: Integration of the control plane of a WiFi provider with a cloud-based AAA service**

Fig. 1 illustrates the integration of the control plane of a WiFi provider with a cloud-based AAA service, per the techniques of this disclosure. A network device (102) of the WiFi provider interacts with the cloud-based AAA service (104) in one of two ways, e.g., registration and operations flow (106), and configuration flow (110).

The network device can be, e.g., an access point, a WiFi gateway, a WiFi network controller, etc. If the device is an access point, it is co-located with the region of WiFi coverage. If the device is a WiFi network controller, e.g., a device that manages several access points, then it need not be co-located with the regions of WiFi coverage. The registration and operations flow is implemented via an API. The configuration flow is implemented via a web application (108) that enables clients to complete registration and management functions via a GUI, e.g. a WiFi provider console.

The registration flow is triggered by a simple mechanism, e.g., by reading a QR code, by checking a box in a web portal, etc., when the network device attempts a first connection to the

cloud-based AAA service. During registration, the network device exchanges certificate and other information with the cloud-based AAA service.

The cloud-based AAA service checks the certificate for validity, and if it finds the certificate to be valid, registers the network device and sends out a configuration URL to the owner or administrator of the WiFi hotspot. The owner or administrator of the WiFi hotspot, who need not be co-located with the hotspot, uses the configuration URL to login, authenticate themselves, and authorize the operation of the hotspot. The administrator also securely fills out basic details about the hotspot, e.g., name, access codes and procedures, look-and-feel of the captive portal of the hotspot, advertising settings, etc., that customize and configure the hotspot. In this manner, credential provisioning is completed quickly, and an auditable trust relationship is established between the smaller WiFi provider and the larger back-end service.

Upon the completion of configuration, the network device and its associated hotspots are ready for operation, e.g., to accept WiFi clients. During operation, client devices associate with the network device, and the network device forwards the clients' access requests to the cloud-based AAA service for authentication, authorization, and accounting purposes.

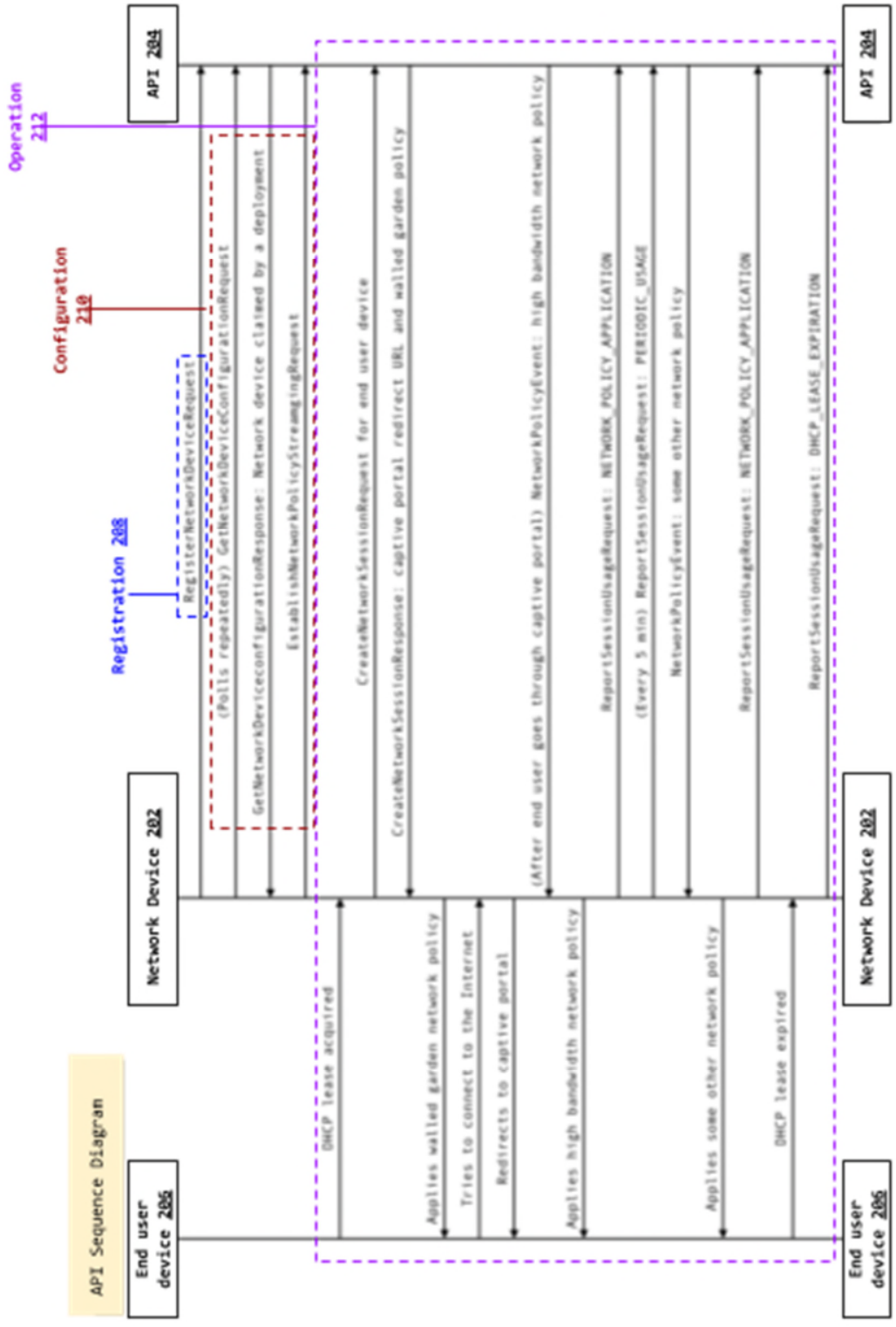


**Fig. 2: Sequence of message exchanges between the cloud-based AAA service, the network device, and the end-user device**

Fig. 2 illustrates the sequence of message exchanges between the cloud-based AAA service (API, 204), the network device (202), and the end-user device (206). As explained before, the message sequence comprises three flows - registration, configuration, and operation.

**Registration**

The registration flow (206), in which a new network device requests registration with the cloud-based AAA and receives a response, can include fields like device ID, a self-signed X.509 certificate, etc. The API receives the registration request and checks if the hash of the client certificate exists in the claim table. If it already exists, the cloud service returns a unique claim URL which points to the web application. If it does not already exist, the cloud service creates a new claim URL and stores the tuple of the certificate and the claim URL.

**Configuration**

Once the network device is registered, the API sends out a configuration URL to the administrator via a web application and receives from the administrator an authorization to operate the hotspot. When the web application is loaded with a claim URL, it checks if the associated client certificate has already been claimed by a WiFi deployment. If it has been claimed, the web front-end displays an error to the user. If it has not been claimed, the user goes through with the claim flow on the web front-end. During the claim flow mentioned in the registration process, after the device is registered successfully, WiFi provider personnel can configure the device using the web application.

During the configuration flow (210) between the network device and the API, the network device polls the API to check if the configuration URL has been filled out by the administrator. It eventually may receive a positive response from the API, e.g., stating that the network device is claimed by a deployment. Along with the authorization to operate, the API

may transmit a policy for network streaming to the network device. The network device is now ready for operation, e.g., ready to serve client devices, which it does by broadcasting its service set identifier (SSID), activating its captive portal, etc.

**Operation**

After device registration and configuration, the vendor network device receives a successful configuration status and establishes a streaming channel to start WiFi service operations (212). The network device is now ready to serve user traffic and provide WiFi services to users by interacting with the cloud-based AAA service via the set of operation APIs. This set of APIs covers the following three operational functionalities.

*Connection state change*

After a streaming channel has been successfully established (as a result of successful device registration), each time an end-user device connects to the local network of the network device, the network device creates a network session to receive a redirect URL to WiFi captive portal, the initial walled garden policy to install for the session, and a session ID that uniquely identifies the session. The network device also reports the DHCP lease expiration event for each end-user device to the cloud-based AAA service, with total session usage statistics attached.

*Policy change*

For active sessions, after receiving a network policy event for a session from the cloud-based AAA service (through the streaming channel) and after applying the policy to the corresponding end-user device, the network device reports the policy change back to the API, with cumulative session usage stats attached. An example of policy change includes terminating a user's WiFi session, changing the network bandwidth for the user session, etc.

*Periodic usage report for accounting*

For active sessions, the network device reports periodic cumulative session usage statistics to the API, for example, once every five minutes.

In this manner, the disclosed vendor-agnostic APIs simplify the integration of the control plane of WiFi network devices with cloud-based AAA services. The time and the cost of the integration process are significantly reduced, as devices can be self-registered and self-configured by WiFi providers, and registration and configuration can be achieved by remote procedure calls via the APIs. As long as the WiFi devices support the APIs as clients, the registration and configuration process is agnostic to device or cloud vendors. The integration process between the local-area and the wide-area service providers is thus accelerated, from the traditional months-long onboarding process to hours or minutes.

## CONCLUSION

This disclosure describes a set of vendor-agnostic application program interfaces (APIs) that enable a WiFi hotspot provider to integrate its control plane with a cloud-based authentication, authorization, and accounting (AAA) service in a self-service manner, without the direct involvement of personnel from the cloud service. This set of APIs enable a WiFi provider to self-register and self-configure its WiFi devices, such as controllers, with the cloud-based AAA service. Once registered and configured, the WiFi device can send requests to the cloud-based AAA service for creating WiFi sessions to control and account for users' network access.

## REFERENCES

[1] Google Station accessed Apr. 22, 2020.