

WLAN Roaming with Wireless Controller, and RADIUS Authentication

Mohit Bajpai

Abstract: *With the increasing adoption of wireless local area networks and the growing demand for seamless mobility, the need for efficient roaming mechanisms has become paramount. This paper presents a comprehensive approach to optimizing WLAN roaming using Mobile IP, Home Agent, Foreign Agent, Wireless Controller, and RADIUS Authentication. The proposed framework addresses the challenges of secure user authentication, seamless handoffs, and integrated billing support across heterogeneous wireless networks. The Wireless Controller plays a crucial role in facilitating WLAN roaming by managing the registration and mobility of mobile nodes, as well as coordinating with the Home Agent and Foreign Agent to ensure uninterrupted connectivity during handoffs.*

Keywords: Wireless LAN, Roaming, Mobile IP, Home Agent, Foreign Agent, RADIUS Authentication, Wireless Controller

1. Introduction

The convergence of wireless technologies, such as cellular networks and wireless local area networks, has enabled mobile users to seamlessly access various network services while on the move [1]. As users transition between different wireless domains, the ability to maintain uninterrupted connectivity and ensure secure access is crucial.

Mobile IP provides a promising solution for enabling seamless roaming across wireless networks by introducing the concepts of Home Agent and Foreign Agent. [2], [3] [4] [1] The Home Agent acts as a proxy for the mobile node, forwarding packets destined for the mobile node to its current location, while the Foreign Agent facilitates the mobile node's registration and packet delivery in the visited network

Wireless LAN Controller is a Key Component in Optimizing Roaming. The Wireless LAN Controller plays a crucial role in the proposed roaming framework. It is responsible for managing the registration and mobility of mobile nodes, as well as coordinating with the Home Agent and Foreign Agent to ensure seamless handoffs. The Wireless LAN Controller is the central point of control and management for the WLAN infrastructure, providing a unified interface for configuring, monitoring, and troubleshooting the wireless network.

Secure User Authentication with RADIUS (AAA) ensuring secure user authentication, it is a critical aspect of the roaming framework. The proposed system leverages RADIUS to authenticate users and authorize their access to the WLAN. The RADIUS server is responsible for verifying user credentials and enforcing access control policies, providing a centralized and scalable authentication mechanism for the wireless network.

The integration of Mobile IP, Home Agent, Foreign Agent, Wireless LAN Controller, and RADIUS Authentication creates a comprehensive solution for optimizing WLAN roaming.

Roaming Architecture

The proposed roaming architecture consists of the following key components: the Mobile Node, which represents the

mobile user device; the Home Agent, which acts as a proxy for the mobile node in its home network; the Foreign Agent, which facilitates the mobile node's registration and packet delivery in the visited network; the Wireless LAN Controller, which manages the registration and mobility of mobile nodes; and the RADIUS server, which handles user authentication and authorization.

Mobile Node

The Mobile Node is the user device that moves between different wireless domains. When the Mobile Node enters a visited network, it registers with the Foreign Agent, which then informs the Home Agent of the mobile node's current location.

Home Agent

The Home Agent is responsible for maintaining the mobile node's permanent address and forwarding packets destined for the mobile node to its current location. The Home Agent acts as a proxy for the mobile node, ensuring that its communication sessions are maintained despite changes in the mobile node's point of attachment to the network.

Foreign Agent

The Foreign Agent is responsible for facilitating the mobile node's registration and packet delivery in the visited network. When a mobile node enters a foreign network, it registers with the Foreign Agent, which then informs the Home Agent of the mobile node's current location.

Wireless LAN Controller

The Wireless LAN Controller is the central point of control and management for the WLAN infrastructure. It is responsible for managing the registration and mobility of mobile nodes, as well as coordinating with the Home Agent and Foreign Agent to ensure seamless handoffs.

The Wireless LAN Controller performs the following key functions:

- 1) Manages the registration and mobility of mobile nodes
- 2) Coordinates with the Home Agent and Foreign Agent to ensure seamless handoffs
- 3) Provides a unified interface for configuring, monitoring, and troubleshooting the wireless network
- 4) Serves as the central point of control and management for the WLAN infrastructure

Volume 7 Issue 6, June 2018

www.ijsr.net

Licensed Under Creative Commons Attribution CC BY

RADIUS Server

The RADIUS server is responsible for authenticating users and authorizing their access to the WLAN. The RADIUS server verifies user credentials and enforces access control policies, providing a centralized and scalable authentication mechanism for the wireless network.

Roaming Workflow

The roaming workflow involves the following steps:

- 1) The mobile node enters a foreign network and detects the availability of a new wireless access point.
- 2) The mobile node registers with the Foreign Agent of the visited network, providing its current location and network address information.
- 3) The Foreign Agent coordinates with the Home Agent to update the mobile node's current location information in the Home Agent's database.
- 4) The Home Agent then transparently forwards packets destined for the mobile node to its new location, facilitated by the Foreign Agent.
- 5) The RADIUS server verifies the mobile node's credentials and enforces the appropriate access policies during the registration process.
- 6) The RADIUS server also updates the user's billing information to enable integrated billing support across the roaming process. As the mobile user moves between different wireless networks, this roaming workflow ensures seamless connectivity and secure access to network services, enabling uninterrupted communication and a high-quality user experience.

Handoff Management

The handoff process in the proposed architecture is designed to minimize service disruption and ensure seamless connectivity. When a mobile node detects the availability of a new network, it initiates the handoff process by registering with the Foreign Agent of the visited network.[3] [1] During this registration, the mobile node provides its current location and network address information to the Foreign Agent.

The Foreign Agent then coordinates with the Home Agent to update the mobile node's current location information in the

Home Agent's database. This ensures that all packets destined for the mobile node are transparently forwarded by the Home Agent to the mobile node's new location, facilitated by the Foreign Agent. This handoff process allows the mobile node to maintain uninterrupted connectivity as it transitions between different wireless networks.

Furthermore, the RADIUS server is responsible for managing the user's access privileges and enforcing any necessary policy updates during the handoff process. The RADIUS server verifies the mobile node's credentials and ensures that the appropriate access policies are applied, enabling a secure and seamless handoff experience for the user.

Security and Billing

The integration of RADIUS authentication within the roaming architecture provides a secure and centralized mechanism for user authentication and authorization. [2] [4] The RADIUS server as part of the AAA framework, maintains a database of user profiles, including their access privileges and billing information. During the roaming process, the RADIUS server verifies the user's credentials and enforces the appropriate access policies.[5]

The use of RADIUS authentication also enables integrated billing support, allowing service providers to track user activities and generate accurate invoices across different wireless networks.

The RADIUS server, as part of the AAA framework, maintains a database of user profiles, including their access privileges and billing information. During the roaming process, the RADIUS server verifies the user's credentials and enforces the appropriate access policies. The use of RADIUS authentication within the AAA system also enables integrated billing support, allowing service providers to track user activities and generate accurate invoices across different wireless networks.

The Figure 1 below shows high level WLAN roaming architecture

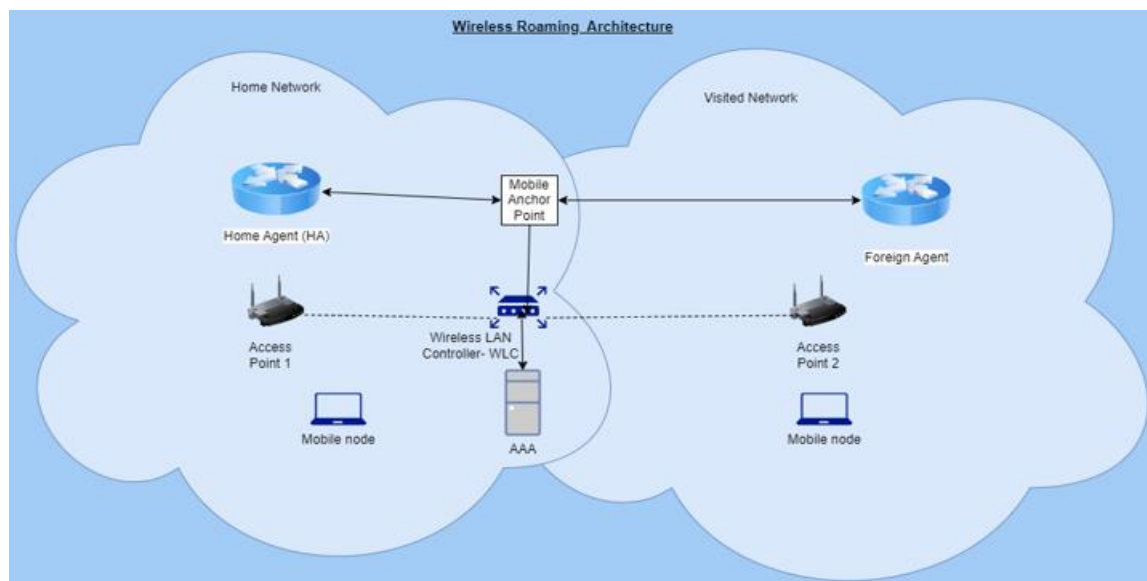


Figure 1

2. Conclusion

This paper has presented a comprehensive approach to optimizing WLAN roaming by leveraging the strengths of Mobile IP, Home Agent, Foreign Agent, and RADIUS Authentication. The proposed framework addresses the challenges of secure user authentication, seamless handoffs, and integrated billing support across heterogeneous wireless networks.

The integration of RADIUS authentication within the roaming architecture provides a secure and centralized mechanism for user authentication and authorization, enabling seamless access control and integrated billing support.

The handoff management process ensures continuous connectivity by coordinating the mobile node's registration with the Foreign Agent and updating the mobile node's current location with the Home Agent.

The proposed approach offers a robust and efficient solution for enabling secure and seamless WLAN roaming, catering to the growing demand for mobile connectivity and ubiquitous access to wireless services.

References

- [1] Kukliński, S., Li, Y., & Dinh, K T. (2014, December 1). Handover management in SDN-based mobile networks. <https://doi.org/10.1109/glocomw.2014.7063430>
- [2] Shi, M., Shen, X., Mark, J., & Zhao, D. (2007, August 14). A versatile roaming service framework with billing support for WLAN/cellular integrated networks. <https://doi.org/10.1145/1577222.1577275>
- [3] Sen, J. (2010, March 1). Mobility and Handoff Management in Wireless Networks. <https://doi.org/10.5772/8482>
- [4] Kinoshita, S., Watanabe, T., Yamasaki, Y., Goto, H., & Sone, H. (2013, July 1). Fault-Tolerant Wireless LAN Roaming System Using Client Certificates. <https://doi.org/10.1109/compsac.2013.137>
- [5] Al-Harthy, K., & Shawkat, W. (2013, November 1). Implement network security control solutions in BYOD environment. <https://doi.org/10.1109/iccsce.2013.6719923>