Koneru Lakshmaiah Education Foundation
(Deemed to be University estd. u/s. 3 of the UGC Act, 1956)
Off-Campus: Bachupally-Gandimaisamma Road, Bowrampet, Hyderabad, Telangana - 500 043.
Phone No: 7815926816, www.klh.edu.in

**Case Study ID:** CS-DHCP-001

## 1. Title- DHCP Snooping in a University Network: Preventing Rogue Attacks and Enhancing Network Security

## 2. Introduction

- Overview

  In this case study, we examine how DHCP snooping was implemented in a large university network to prevent rogue DHCP attacks and improve overall network security. The primary objective was to secure the dynamic IP address allocation process and protect users from unauthorized devices and network interference.
- Objective

  The main goal of this study is to analyze the deployment of DHCP snooping in the university's network to prevent rogue DHCP servers from assigning malicious IP addresses, which could lead to network disruptions and data interception.

## 3. Background

- Organization/System /Description

  The university has a sprawling campus network that supports thousands of users, including students, faculty, and administrative staff. The network provides internet access via both wired and wireless connections, with several subnetworks for academic departments, public access points, and administrative offices.
- Current Network Setup

  Network Type: Ethernet-based with VLAN segmentation for different user groups

  DHCP Architecture: Centralized DHCP server that manages dynamic IP

  address assignments across various VLANs.
- Security

  Prior to DHCP snooping implementation, the network had basic firewall encryption for wireless traffic but lacked mechanisms to monitor DHCP-related activities.

## 4. Problem Statement

- Challenges Faced

The university began experiencing network disruptions and intermittent connectivity issues caused by rogue DHCP servers, often inadvertently introduced by students connecting personal routers or unauthorized devices. These rogue servers issued incorrect IP addresses, leading to:IP address conflicts,Network outages,Potential for data interception by malicious actors redirecting network traffic.The absence of DHCP snooping or other similar security measures made it difficult to detect and prevent these rogue DHCP attacks

## 5. Proposed Solutions

- Approach

To address these challenges, the university's IT team proposed the deployment of **DHCP snooping** as a method to monitor and control DHCP traffic, ensuring that only authorized DHCP servers could assign IP addresses within the network.

- Technologies/Protocols Used

**DHCP Snooping**: A Layer 2 security feature that filters DHCP messages on untrusted ports.

**VLAN Segmentation**: To further isolate network traffic and reduce the attack surface.

**Switch Configuration**: Enable snooping on all access switches to filter out unauthorized DHCP messages.

**IP Source Guard**: Ensures that traffic is only allowed from valid IP addresses based on DHCP leases.

## 6. Implementation

- Process

The implementation followed these steps:

**Network Audit**: Assess existing switch configurations and map out the VLAN structure to determine where DHCP snooping needs to be enabled.

**Configure DHCP Snooping**: Activate DHCP snooping on all Layer 2 switches in the network, marking trusted ports where the legitimate DHCP servers reside.

**Enable IP Source Guard**: Protect against spoofing by tying IP addresses to specific MAC addresses on the network.

**Monitoring**: Deploy monitoring tools to log and alert on any suspicious DHCP traffic.

- Implementation

**Switch Configuration**: Configured trusted ports for DHCP servers on the core switches and untrusted ports on edge switches.

**Testing**: Introduced controlled rogue DHCP scenarios to test whether the snooping feature blocked unauthorized DHCP responses.

- **Timeline**

**Phase 1 (1 Month)**: Network audit and VLAN assessment.

**Phase 2 (1 Month)**: Switch configuration and activation of DHCP snooping.

**Phase 3 (1 Month)**: Testing and monitoring deployment.

## 7. Results and Analysis

- Outcomes

**Improved Network Stability**: IP conflicts and rogue server issues were completely eliminated, resulting in stable network performance.

**Enhanced Security**: No unauthorized devices could serve DHCP addresses, reducing the risk of man-in-the-middle (MITM) attacks.

**User Satisfaction**: Complaints regarding network connectivity issues significantly decreased, particularly in student dormitory areas.

- **Analysis**

**Network Traffic**: Monitoring tools showed a marked reduction in rogue DHCP traffic and improved IP address assignment accuracy.

**System Performance**: The implementation of DHCP snooping introduced negligible overhead on network performance while significantly boosting security.

## 8. Security Integration

- Security Measures

**Trusted/Untrusted Port Configuration**: By designating only trusted ports for authorized DHCP servers, the network reduced the chance of rogue DHCP servers gaining control.

**IP Source Guard**: This additional layer ensured that IP spoofing attacks were thwarted by validating the source IP address against the DHCP database.

**Monitoring**: Continuous monitoring of DHCP traffic ensured that any attempts to introduce rogue DHCP servers were quickly detected and neutralized.

## 9. Conclusion

- Summary

The implementation of DHCP snooping in the university network successfully prevented rogue DHCP servers from disrupting operations and enhanced overall network security. The use of additional features like IP Source Guard further solidified the defense against DHCP-related attacks.

## 10. References

**Citations :[1] Reference Research papers,** "Network Security Essentials: Applications and Standards" by William Stallings, • [2] Johnson, M., & Wang, P. (2019). Next-Generation Firewalls: Applications in School Systems. Cybersecurity Review, 8(4), 102-110. • [3] Patel, A., & Kaur, R. (2020). Content Filtering in Education. International Journal of IT & Security, 12(6), 25-38.

**NAME:**Sajjan Samanvitha

**ID-NUMBER:**2320030437

**SECTION-NO:**7