STATE OF CALIFORNIA
FAIR POLITICAL PRACTICES COMMISSION
1102 Q St. · Suite 3050 · Sacramento, CA 95811
(866) 275-3772

ARPWATCH

CONFIGURATION

System: Internal Ubuntu 18.04.06 VM

Date: May 28, 2025

OUTLINE

This document outlines the configuration of ARPWatch on the Ubuntu 18.04.6 virtual machine deployed on a host server. The purpose of this setup is to monitor Ethernet-based device connections and send real-time email alerts using `ssmtp` with Gmail SMTP authentication.

INTRODUCTION

ARPWatch has been configured on an Ubuntu 18.04.6 Virtual Machine hosted to monitor MAC/IP activity on the `eth0` interface. The goal of this project is to provide real-time visibility into new or changed devices on the network.

Email alerts are sent using `ssmtp` with a dedicated Gmail account authenticated via SMTP. This document records the configuration for reference and documentation.

SYSTEM DETAILS

Component	Value
Host Server	*(internal virtual host)*
Virtual Machine	*(Ubuntu-based VM)*
OS	Ubuntu 18.04.06 (Server Install Image)
Network Interface	eth0
Monitoring Tool	arpwatch
Mail Agent	ssmtp
Alert Recipient	*(internal sysadmin email)*
SMTP Auth Email	*(internal Gmail email)*

CONFIGURATION OVERVIEW

Package Installation

ARPWatch and sSMTP were installed via `apt` on the virtual machine to monitor Ethernet connections and send email alerts. The following configuration steps detail the service setup and mail relay settings. The following packages were installed:

```
apt install arpwatch ssmtp
```

ARPWatch Service

Check Service Status:

```
systemctl status arpwatch@eth0
```

Start Service Manually:

```
systemctl start arpwatch@eth0
```

Restart Service after Changes:

```
systemctl restart arpwatch@eth0
```

Stop Service:

```
systemctl stop arpwatch@eth0
```

sSMTP Configuration

Email alerts from ARPWatch are sent using Gmail's SMTP server via sSMTP. The sending address is used to dispatch alerts, while the delivery address receives them.

Path to Config File: /etc/ssmtp/ssmtp.conf

```
root=alerts@example.com
mailhub=smtp.gmail.com:587
hostname=arpwatch-vm
UseTLS=Yes
UseSTARTTLS=Yes
AuthUser=your.alerts@gmail.com
AuthPass=[App Password]
FromLineOverride=YES
```

Path to Revaliases File: /etc/ssmtp/revaliases

```
arpwatch:alerts@example.com:smtp.gmail.com:587
```

TESTING & VALIDATION

ARPWatch Functionality

To verify ARPWatch is running and detecting new devices, the following log command can be used:

```
tail -f /var/log/syslog | grep arpwatch
```

Expected Output:

```
May 29 20:07:25 hostname arpwatch: new station 192.168.153.170b8:31:b5:32:31:03 eth0

May 29 20:12:23 hostname arpwatch: new station 192.168.153.144 a0:4a:5e:c8:f6:80 eth0
```

Email Alert Delivery

Email Functionality verifies at the SMTP events in the same log:

```
May 29 20:03:54 hostname sSMTP[10431]: Sent mail for arpwatch@ hostname (221 2.0.0 closing connection ...)

May 29 20:07:28 hostname sSMTP[10432]: Sent mail for arpwatch@ hostname (221 2.0.0 closing connection ...)

May 29 20:12:26 hostname sSMTP[10435]: Sent mail for arpwatch@ hostname (221 2.0.0 closing connection ...)
```

MAINTENANCE & SECURITY NOTES

ARP Database

The ARPWatch Database is stored at:

```
/var/lib/arpwatch/eth0.dat
```

To get a clean copy of the database to retrigger alerts for existing devices (for testing), stop the service and delete the file:

```
systemctl stop arpwatch@eth0

rm /var/lib/arpwatch/eth0.dat
```

Note: Do not open the eth0.dat file in nano and clear its contents as this will not retrigger alerts. The file must be fully deleted for ARPWatch to treat previously seen devices as new.

Email Password Security

The Gmail password used in `/etc/ssmtp/ssmtp.conf` should be an App Password and not a standard account password.

Log Monitoring

All ARPWatch and mail activity is logged in `/var/log/syslog`. You can tail this log to observe both detection and email relay activity.

For service-level logs (including errors, restarts, or status changes):

```
journalctl -u arpwatch@eth0
```