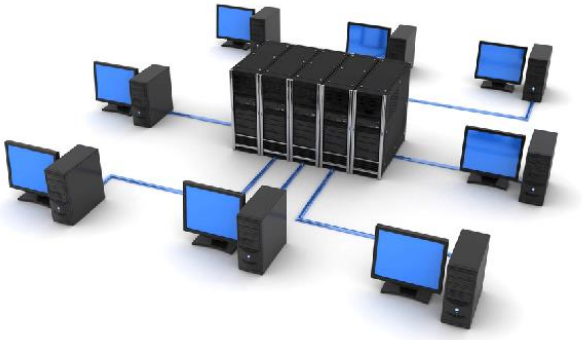
Network Monitoring Compliance Database

By: Harrison Brown

Problem

- On a large computer network like the one at UC Merced, security gets harder with the number of devices connected
- Some kind of monitoring system is needed to secure the network
- For this project, the task was to create a monitoring system that keeps track of device metadata and device manufacturer
- This system needs to stay up to date and store data



Solution: In Three Parts

1. Getting connected devices
2. An SQL database
3. Periodic updates

Getting Connected Devices

- A list of unique device addresses (MAC addresses) was retrieved from the Address Resolution Protocol (ARP) tables of a network switch
- ARP table was downloaded by running commands over a remote terminal (SSH) and parsing the output

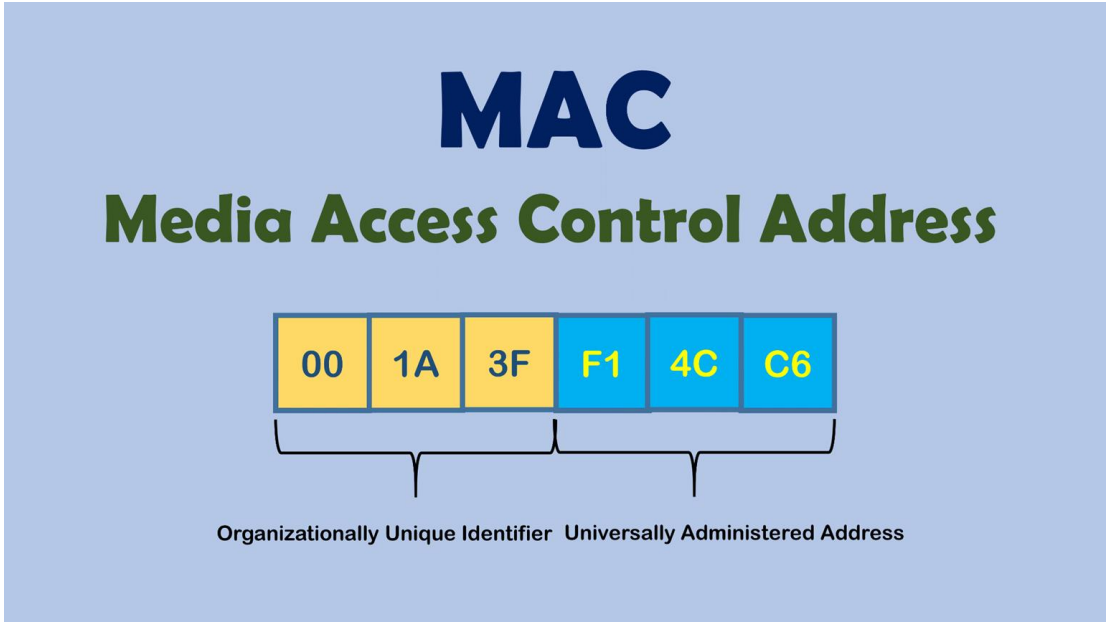
Total number of ARP entries: 542
(In all VRFs)

	IP Address	MAC Address	Type	Age	Port/ Port (Vpls-Id, Vlan)/ Vpls-Id:Peer
1	169.236.138.120	e4e7.4903.507c	Dynamic	1	2/1
2	10.42.3.80	cc4e.24f4.61e8	Dynamic	2	2/7
3	169.236.138.129	None	Pending	0	v1138
4	169.236.138.131	None	Pending	0	v1138
5	169.236.138.132	None	Pending	0	v1138
6	10.42.3.90	cc4e.24f3.e0a8	Dynamic	0	1/9
7	169.236.146.150	None	Pending	0	v1146
8	10.42.3.100	cc4e.24f4.6a28	Dynamic	0	2/9
9	10.42.3.110	cc4e.24d1.5880	Dynamic	2	2/9
10	10.42.3.111	cc4e.24d1.5200	Dynamic	0	2/9
11	169.236.138.156	04bd.88ca.7cd4	Dynamic	2	2/1
12	169.236.138.160	0014.a002.18a3	Dynamic	1	2/1
13	169.236.50.3	cc4e.2493.d800	Dynamic	0	1/17
14	169.236.50.13	None	Pending	0	v1050
15	169.236.146.193	a0ce.c8e3.71ef	Dynamic	1	2/7
16	169.236.138.184	3ccd.3661.6f2c	Dynamic	2	2/1
17	169.236.50.36	None	Pending	0	v1050
18	169.236.50.41	None	Pending	0	v1050

An ARP table holds a device's network address (IP) and unique device address (MAC). The example to the left is from a network switch.

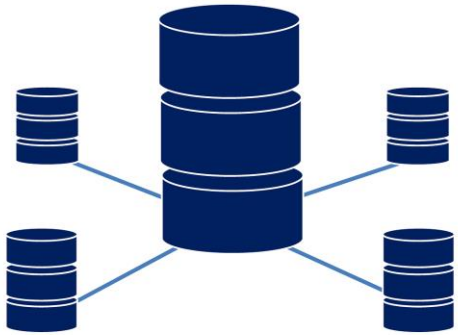
Using Device Addresses to find the Manufacturer

- Each device manufacturer found use an IEEE MAC address prefix table
- This table will tell you organizational identifier is owned by which company



The SQL Database

- The specific database used was an installation of Oracle Database installed on a virtual machine connected to the university network
- The ARP table was in text format so I made use of external tables, an oracle feature for querying raw text files



	MAC	IP	MANUFACTURER	MODIFIED_AT	FOUND_AT
1	e0:db:55:23:ab:52	169.236.151.201	Dell Inc.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
2	00:19:b9:b5:97:a5	169.236.151.202	Dell Inc.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
3	00:19:b9:b5:b5:0a	169.236.151.211	Dell Inc.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
4	08:00:37:42:a9:3b	169.236.151.250	FUJI-XEROX CO. LTD.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
5	cc:4e:24:93:d8:00	169.236.152.3	Brocade Communications Systems LLC	25-FEB-21 05.52.46.384687000 AM	20-FEB-21 05
6	cc:4e:24:93:d8:00	169.236.144.3	Brocade Communications Systems LLC	20-FEB-21 06.59.10.137695000 PM	20-FEB-21 05
7	cc:4e:24:93:d8:00	169.236.136.3	Brocade Communications Systems LLC	25-FEB-21 01.47.17.104836000 AM	20-FEB-21 05
8	cc:4e:24:93:d8:00	169.236.128.3	Brocade Communications Systems LLC	20-FEB-21 06.59.10.137695000 PM	20-FEB-21 05
9	24:4b:fe:59:52:45	169.236.152.60	ASUSTek COMPUTER INC.	26-FEB-21 11.07.26.018187000 AM	20-FEB-21 05
10	78:7b:8a:c5:99:b8	169.236.136.92	Apple, Inc.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
11	b8:ca:3a:bc:c2:91	169.236.152.122	Dell Inc.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
12	64:00:6a:5b:2d:9e	169.236.144.107	Dell Inc.	26-FEB-21 10.52.24.496669000 AM	20-FEB-21 05
13	d8:cb:8a:c1:76:21	169.236.152.141	Micro-Star INTL CO., LTD.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
14	54:42:49:e2:3e:fb	169.236.136.112	Sony Corporation	26-FEB-21 11.07.26.018187000 AM	20-FEB-21 05
15	2c:f0:5d:1b:9c:8e	169.236.144.132	Micro-Star INTL CO., LTD.	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05
16	ac:16:2d:08:11:7a	169.236.144.140	Hewlett Packard	26-FEB-21 10.57.25.115777000 AM	20-FEB-21 05
17	3c:70:59:02:6e:3d	169.236.136.131	MakerBot Industries	26-FEB-21 11.07.26.018187000 AM	20-FEB-21 05
18	40:61:86:e1:05:86	169.236.128.118	MICRO-STAR INT'L CO.,LTD	26-FEB-21 11.12.27.099103000 AM	20-FEB-21 05

Periodic Updates

- Devices are always connecting and disconnecting from the wifi, so updating the data is important
- A simple but important part of the project was keeping the database up to date
- This was done by running scripts in a cron job which allows for code to be run at any interval

Issues

- Automating shell commands
  - I basically needed to run a terminal inside a remote terminal and enter passwords without actually entering them with my keyboard
  - The solution I found was to use a scripting language called Expect that allocates a pseudo terminal that will automatically type passwords and execute commands for me.

What I learned

- Oracle
  - How to install an Oracle database
  - Oracle specific SQL features
- MAC address prefixes
- Over complicated solutions are always bad
  - I started out by writing way too much code
  - I received one tip that greatly reduced the complexity of my solution

What Next?

- Portability
  - The project installation is quite involved and is difficult to move to another computer
- Moving beyond bash scripts
  - Many people love bash scripts but they can be buggy and slightly unreliable compared to a fully fledged programming language
  - A lot of this project was written in bash and would benefit from a re-write in a more reliable language
- Other scheduling programs for periodic updates
  - I used cron jobs but there are other options
  - Systemd timers or the Oracle Job Scheduler are two options that might be more flexible for different scheduling needs
- A front-end web interface

Questions?

Image Sources:

- https://medium.com/@lakshanmamalgaha/what-is-a-mac-address-and-why-you-should-know-about-it-9f970b3ba3fd
- https://tophat.network/networking/
- https://www.stackery.io/blog/using-relational-databases-with-serverless-functions