

A FAUCET-driven Network Access Control Solution

It's not wise to upset a Wookiee

Problem

- Limit Access to Network Resources
- Credential-specific Resource Restrictions
- Deployable Across the Network
- Working in an SDN Environment
- No Current NAC Solution for Faucet

What is Chewie?

Chewie is:

- EAP / 802.1x Authenticator
- Speaks RADIUS to Authentication Server
- Speaks EAPoL to Supplicant devices
- Provides Credential-based Access Control for Faucet



Why Deploy Chewie?

- Protect LAN Resources
- Credential-specific Policies
- Support for all major EAP-methods (in theory)
- IoT Support with MAB
- Easy to Deploy in Faucet Networks
- Fine-Grained Access Control



Background

Glossary

EAP - Framework for Authentication Protocols

Ensuring common functionality and negotiation of EAP methods

EAP Method - The method used to achieve authentication. (EAP-TLS, PEAP, ...)

NOTE: This is not a line-protocol and must be encapsulated

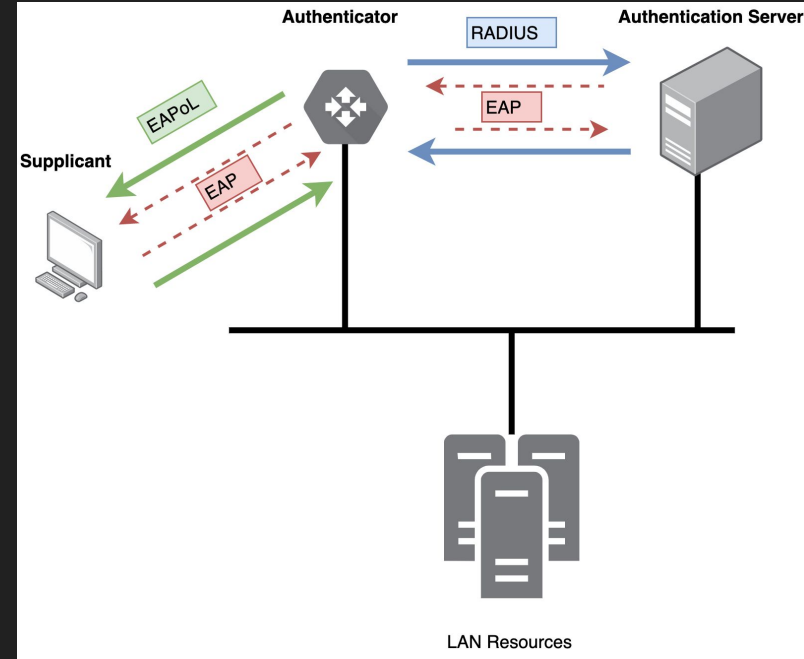
EAPoL - Line-Protocol for Encapsulating EAP-methods over IEEE 802

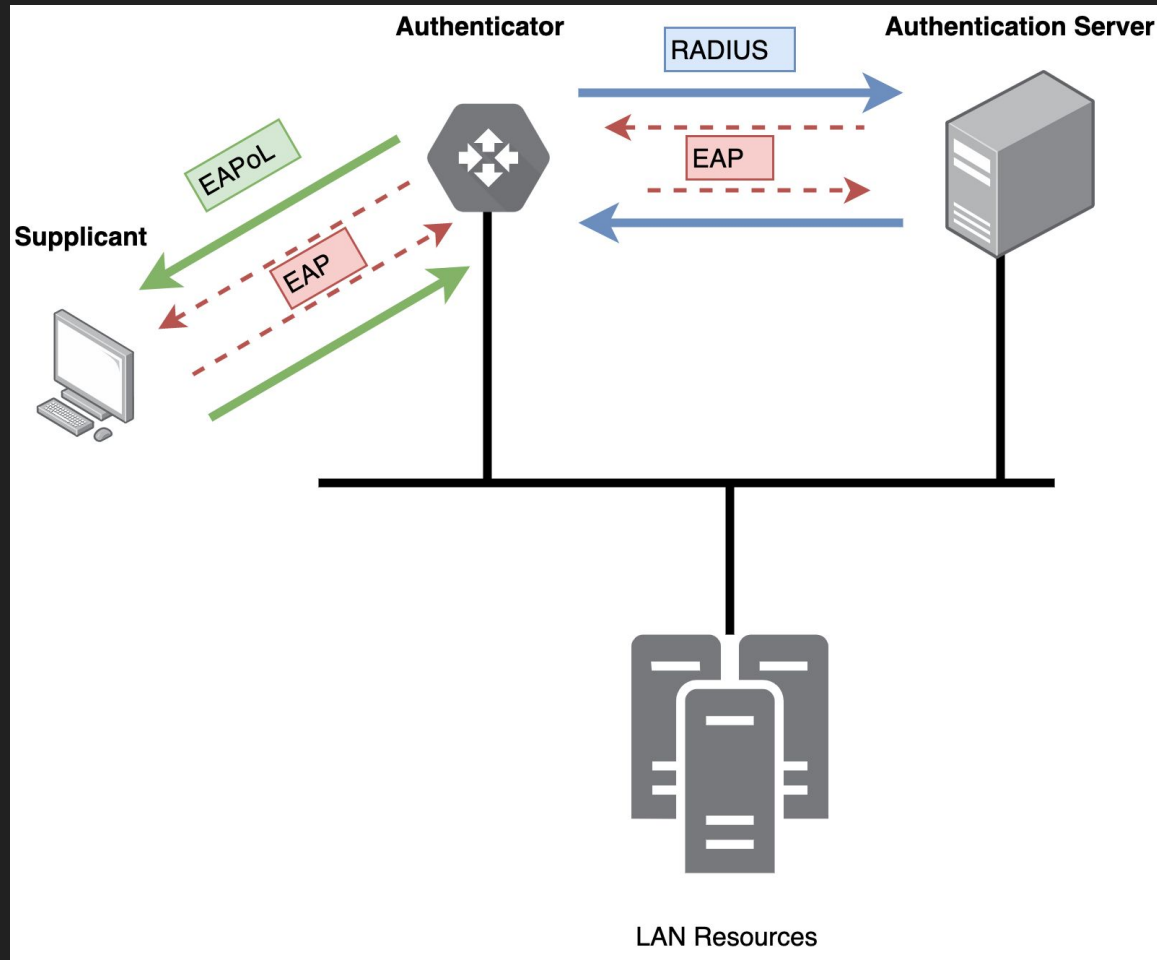
RADIUS - AAA Protocol with EAP Support for Authentication

Mac Authentication Bypass (MAB) - MAC-based Authentication provided by 802.1x Authenticator

Chewie's Power

- RADIUS-Powerhouse
- Translate EAPoL → RADIUS
- Radius Performs EAP Methods
- Avoid Complex Code





User Management

Storing Credentials

- Credentials are Stored in RADIUS
- Can be backed by LDAP
- Users have Restriction Policies Attached

Storing Credentials - RADIUS

```
1  user  Cleartext-Password := "microphone"
2      Session-timeout = {0}
3  admin  Cleartext-Password := "megaphone"
4      Session-timeout = {0}
5  vlanuser1001  Cleartext-Password := "password"
6      Tunnel-Type = "VLAN",
7      Tunnel-Medium-Type = "IEEE-802",
8      Tunnel-Private-Group-id = "radiusassignedvlan1"
9  vlanuser2222  Cleartext-Password := "milliphone"
10      Tunnel-Type = "VLAN",
11      Tunnel-Medium-Type = "IEEE-802",
12      Tunnel-Private-Group-id = "radiusassignedvlan2"
13  filter_id_user_accept  Cleartext-Password := "accept_pass"
14      Filter-Id = "accept_acl"
15  filter_id_user_deny  Cleartext-Password := "deny_pass"
16      Filter-Id = "deny_acl"
```

Providing Filter Policies

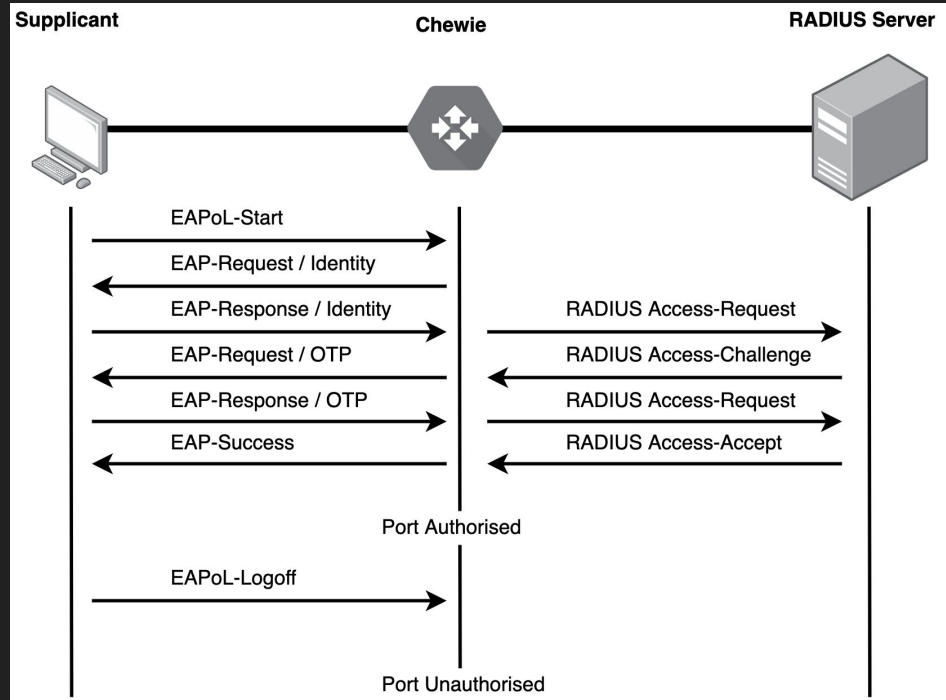
- RADIUS Provides AAA Attributes
 - IETF 64 - Tunnel Type
 - IETF 81 - Tunnel Private Group ID
 - IETF 11 - Filter-Id

Used for Allocation of Dynamic VLANs and ACLs on Authentication Event

Authentication Overview

Performing EAP Authentication

EAP Authentication (Supplicant Software Required)



In Practice?

```
0:50:04 faucet.Chewie INFO Sending message 'IdentityMessage': src_mac: '01:80:c2:00:00:03', id: '94',
0:50:04 faucet.Chewie INFO Sending message 'IdentityMessage': src_mac: '01:80:c2:00:00:03', id: '98',
0:50:19 faucet.Chewie INFO Received eap message: 'EapolStartMessage': src_mac: '56:3d:75:34:7d:31', id:
0:50:19 faucet.Chewie INFO Sending message 'IdentityMessage': src_mac: '56:3d:75:34:7d:31', id: '85',
0:50:19 faucet.Chewie INFO Received eap message: 'IdentityMessage': src_mac: '56:3d:75:34:7d:31', id:
0:50:19 faucet.Chewie INFO Sending Radius Packet. Mac <class 'chewie.mac_address.MacAddress'> 56:3d:75:34:7d:31
0:50:19 faucet.Chewie INFO Sending to RADIUS payload {'src_mac': MacAddress.from_string("56:3d:75:34:7d:31")}
0:50:19 faucet.Chewie INFO sent radius message.
0:50:19 faucet.Chewie INFO Received RADIUS message: <chewie.radius.RadiusAccessChallenge object at 0x7f3b950e60b8>
0:50:19 faucet.Chewie INFO Sending message 'Md5ChallengeMessage': src_mac: 'None', id: '86', code: '1'
00:00:00:00:07 to 56:3d:75:34:7d:31
0:50:19 faucet.Chewie INFO Received eap message: 'Md5ChallengeMessage': src_mac: '56:3d:75:34:7d:31',
    'b''
0:50:19 faucet.Chewie INFO Sending Radius Packet. Mac <class 'chewie.mac_address.MacAddress'> 56:3d:75:34:7d:31
0:50:19 faucet.Chewie INFO Sending to RADIUS payload {'src_mac': MacAddress.from_string("56:3d:75:34:7d:31"), 'extra_data': b''} with state {'data_type': <chewie.radius_datatypes.String object at 0x7f3b950e60b8>}
0:50:19 faucet.Chewie INFO sent radius message.
0:50:19 faucet.Chewie INFO Received RADIUS message: <chewie.radius.RadiusAccessAccept object at 0x7f3b950e60b8>
0:50:19 faucet INFO Success from MAC 56:3d:75:34:7d:31 on 7
0:50:19 faucet.Chewie INFO Sending message 'SuccessMessage': src_mac: 'None', id: '86' from 00:00:00:00:00:00
```

What about IoT?

Not all Clients are able to perform EAP Authentication

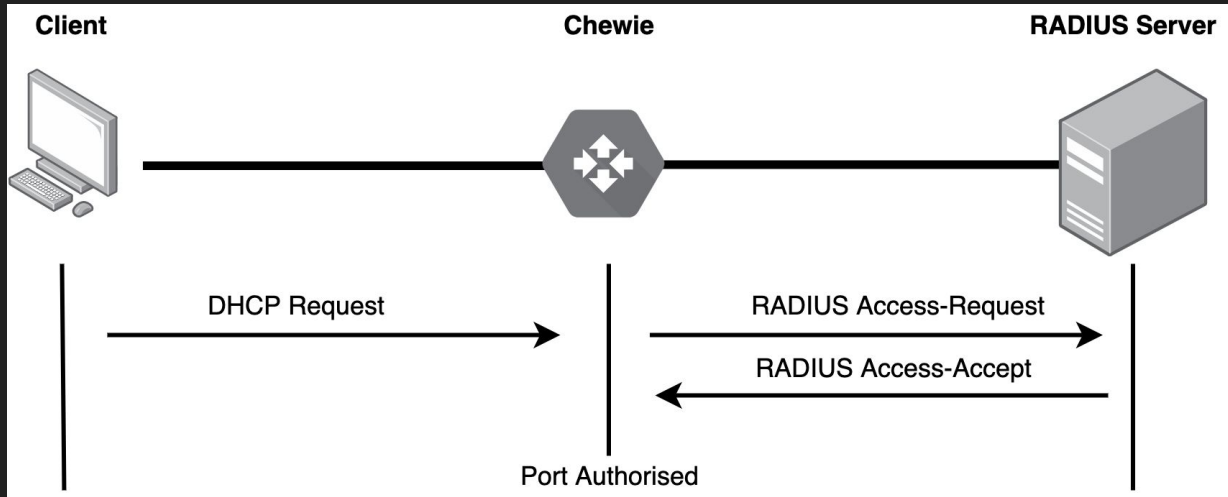
Why build a secure network if we must open ports for phones / printers?

No 'extra' Client Software Required

Mac Authentication Bypass

MAC-based Authentication performed by 802.1x Authenticator

No 'extra' Client Software Required



In Practice?

DHCP Packet is Received by the Authenticator

MAC Address is copied from DHCP Request and Sent to RADIUS Server as Access-Request

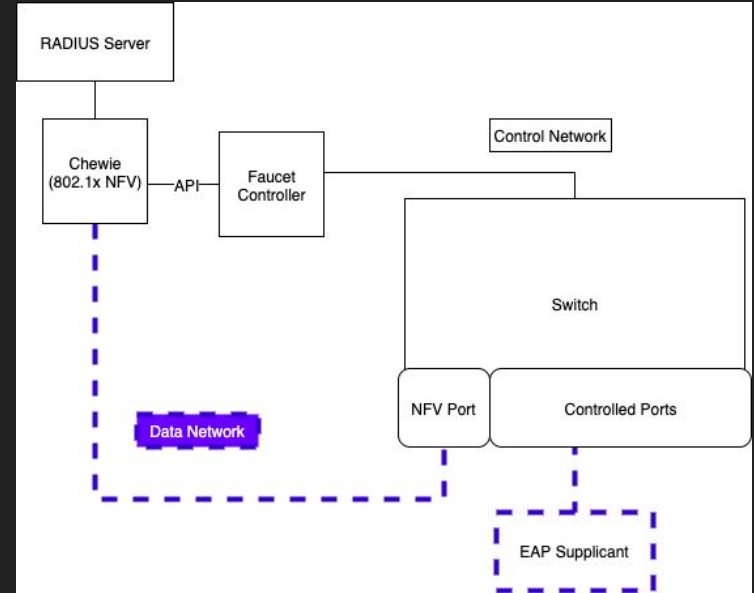
Result is Received by the Authenticator to Authorise Port

```
8:45 faucet.Chewie INFO      Sending message 'IdentityMessage': src_mac: '01:80:c2:00:00:03', id: '33', code: '1', identity:
8:45 faucet.Chewie INFO      Sending message 'IdentityMessage': src_mac: '01:80:c2:00:00:03', id: '42', code: '1', identity:
9:28 faucet.Chewie INFO      Received DHCP packet for MAB. packed message: b'\x00\x00\x00\x00\x00\x06Zrs\xbb\x9e\x87\x08\x00
9:28 faucet.Chewie INFO      Sending MAC to MAB State Machine: 5a:72:73:bb:9e:87
9:28 faucet.Chewie INFO      Sending Radius Packet. Mac <class 'chewie.mac_address.MacAddress'> 5a:72:73:bb:9e:87, Username:
9:28 faucet.Chewie INFO      Sending MAB to RADIUS: 5a:72:73:bb:9e:87
9:28 faucet.Chewie INFO      sent radius message.
9:28 faucet.Chewie INFO      Received RADIUS message: <chewie.radius.RadiusAccessAccept object at 0x7f3ae91540f0>
9:28 faucet INFO      Success from MAC 5a:72:73:bb:9e:87 on 6
```

Chewie Architecture

Network Layout

- NFV Port
- Connected to Faucet
 using Callbacks / Events (BAD)
- Future development for
 gRPC connection (GOOD)
- Allow for both 802.1x and
 non-802.1x Ports



Faucet - Chewie API

Faucet → Chewie

- Port Up
- Port Down

Chewie → Faucet

- Successful Auth Event
- Failed Auth Event
- Logoff Event

Granular Access Control

Providing Filter Policies

- RADIUS Provides AAA Attributes
 - IETF 64 - Tunnel Type
 - IETF 81 - Tunnel Private Group ID
 - IETF 11 - Filter-Id

Used for Allocation of Dynamic VLANs and ACLs on Authentication Event

Allocation of VLANs / ACLs

Chewie supports deployment of ACLs based on user credentials

Default ACLs for all users

VLAN allocation based on credential

No 'downloadable ACLs'

```
1  user  Cleartext-Password := "microphone"
2      Session-timeout = {0}
3  admin Cleartext-Password := "megaphone"
4      Session-timeout = {0}
5  vlanuser1001 Cleartext-Password := "password"
6      Tunnel-Type = "VLAN",
7      Tunnel-Medium-Type = "IEEE-802",
8      Tunnel-Private-Group-id = "radiusassignedvlan1"
9  vlanuser2222 Cleartext-Password := "milliphone"
10     Tunnel-Type = "VLAN",
11     Tunnel-Medium-Type = "IEEE-802",
12     Tunnel-Private-Group-id = "radiusassignedvlan2"
13  filter_id_user_accept Cleartext-Password := "accept_pass"
14     Filter-Id = "accept_acl"
15  filter_id_user_deny Cleartext-Password := "deny_pass"
16     Filter-Id = "deny_acl"
```


Chewie Notes:

Chewie:

- can run independent of Faucet
- is a different project from Faucet
- currently MUST run on Controller Device due to API restrictions

Using Chewie

Chewie Configuration

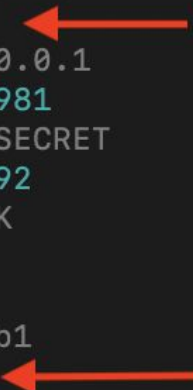
- Configuration is achieved through the `Faucet.yaml` file
- Options include:
 - RADIUS Server
 - Default ACLs for Managed Ports
 - NFV Port Location
 - Marking Ports as Chewie-Managed

NOTE: Faucet Configuration is NOT Changed by Chewie

Getting Set Up

1. Ports are Marked with dot1x
2. Relevant Flows are Created
3. All EAPoL Traffic is forwarded to NFV
All other Traffic is Denied
4. Port is Opened on Successful Auth

```
26 dps:
27   faucet-1:
28     cookie: 2780024671107954022
29     dot1x:
30       nfvp_intf: u024-eth0
31       nfvp_sw_port: 3
32       radius_ip: 127.0.0.1
33       radius_port: 40981
34       radius_secret: SECRET
35     dp_id: 491645073792
36     hardware: CiscoC9K
37     interfaces:
38       1:
39         description: b1
40         dot1x: true
41         dot1x_dyn_acl: true
42         name: b1
43         native_vlan: 100
```



Try it Yourself?

Starting with Chewie

Use Docker...

Seriously...

```
`cd ./chewie && docker-compose up --build`
```

If You're Interested

There are a number of example configurations available in the Faucet Documentation, describing how to introduce Chewie into a Faucet network.

<https://readthedocs.org/projects/faucet/>

Chewie also has developer documentation available below:

<https://readthedocs.org/projects/chewie/>

Adding to a Faucet Deployment

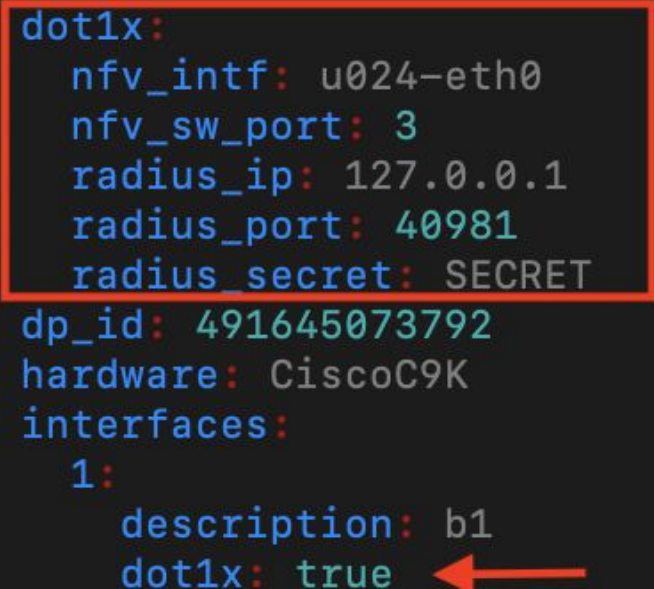
Chewie required the following to be defined in the config file:

- Dot1x section under Data Plane section
- (At least) 1 Port Marked with Dot1x flag

FAUCET will know to run Chewie if defined correctly

Example Base Configuration

```
26 dps:
27     faucet-1:
28         cookie: 2780024671107954022
29         dot1x:
30             nfv_intf: u024-eth0
31             nfv_sw_port: 3
32             radius_ip: 127.0.0.1
33             radius_port: 40981
34             radius_secret: SECRET
35         dp_id: 491645073792
36         hardware: CiscoC9K
37         interfaces:
38             1:
39                 description: b1
40                 dot1x: true
```



Logging / Debugging Network

Verbose Logging in Chewie

Logs are Added to the Faucet Log

All Events are logged in Chewie, including port_up, port_down, authentication_attempts, and all packets received and set are logged.

```
Jul 16 00:50:51 faucet.Chewie INFO Sending message 'IdentityMessage': src_mac: '01:80:c2:00:00:03', id: '141', code: '1', identity: '' from 00:00:00:00:00:07 to 01:80:c2:00:00:03
Jul 16 00:50:51 faucet.Chewie INFO Sending Radius Packet. Mac <class 'chewie.mac_address.MacAddress'> 56:3d:75:34:7d:31, Username: user
Jul 16 00:50:51 faucet.Chewie INFO Sending to RADIUS payload {'src_mac': MacAddress.from_string("56:3d:75:34:7d:31"), 'message_id': 141, 'code': 2, 'identity': 'user'} with state None
Jul 16 00:50:51 faucet.Chewie INFO sent radius message.
Jul 16 00:50:51 faucet.Chewie INFO Sending message 'Md5ChallengeMessage': src_mac: 'None', id: '142', code: '1', challenge: 'b'\xd0p\xac\xa7\x95|\xd9\x89JK\xee\x91\xe3T\x10\xa6'', extra_data: 'b'' fr
om 00:00:00:00:00:07 to 56:3d:75:34:7d:31
Jul 16 00:50:51 faucet.Chewie INFO Sending Radius Packet. Mac <class 'chewie.mac_address.MacAddress'> 56:3d:75:34:7d:31, Username: user
Jul 16 00:50:51 faucet.Chewie INFO Sending to RADIUS payload {'src_mac': MacAddress.from_string("56:3d:75:34:7d:31"), 'message_id': 142, 'code': 2, 'challenge': 'b'Z\x81KQH\xa5\xb7d4\xa94\xb93\xea\xae\
xb4', 'extra_data': 'b''} with state {'data_type': <chewie.radius_datatypes.String object at 0x7f3b950e6a90>}
Jul 16 00:50:51 faucet.Chewie INFO sent radius message.
Jul 16 00:50:51 faucet INFO Success from MAC 56:3d:75:34:7d:31 on 7
Jul 16 00:50:51 faucet.Chewie INFO Sending message 'SuccessMessage': src_mac: 'None', id: '142' from 00:00:00:00:00:07 to 56:3d:75:34:7d:31
```

If You're Stuck - Contact Us

There are a number of mailing lists available to help:

faucet-users@lists.geant.org

faucet-dev@list.waikato.ac.nz

faucet-announce@list.waikato.ac.nz

faucetapps-dev@list.waikato.ac.nz

Overview

Achieved Goals

Applying User-Based Access Restrictions

Providing Port Security for 'Dumb' Clients

No Vendor-Specific Requirements

The Dream that Failed (so far...)

Building Dynamic ACLs from RADIUS Attributes

```
L5
L6 # Using the HPE ACE standard
L7 # http://h22208.www2.hpe.com/eginfolib/networking/docs/swit
L8 filter_rule    Cleartext-Password := "microphone"
L9             NAS-Filter-Rule = "deny in tcp from any to any"
L10
L11
L12
L13
L14
L15
L16
L17
L18
L19
L20
L21 # MAB Examples for integration tests
L22 8e0000000102 Cleartext-Password := '8e0000000102'
L23             NAS-Filter-Rule = "deny in tcp from any to any"
```

Plead for Developers

Implement Co-Processor Compliance

Maintain State on Restart

Integration with Faucet Agent and gRPC / Protobuffers for abstraction

Traverse Multiple Switches to an NFV port

Encrypted Channels using NFV Co-Processors

Questions?

About Me

Michael Washer

Masters Student in Cyber Security

WAND - Waikato University

<https://github.com/MichaelWasher/>

<https://www.linkedin.com/in/michael-washer/>

