aruba
a Hewlett Packard Enterprise company

Mobility Day 2019

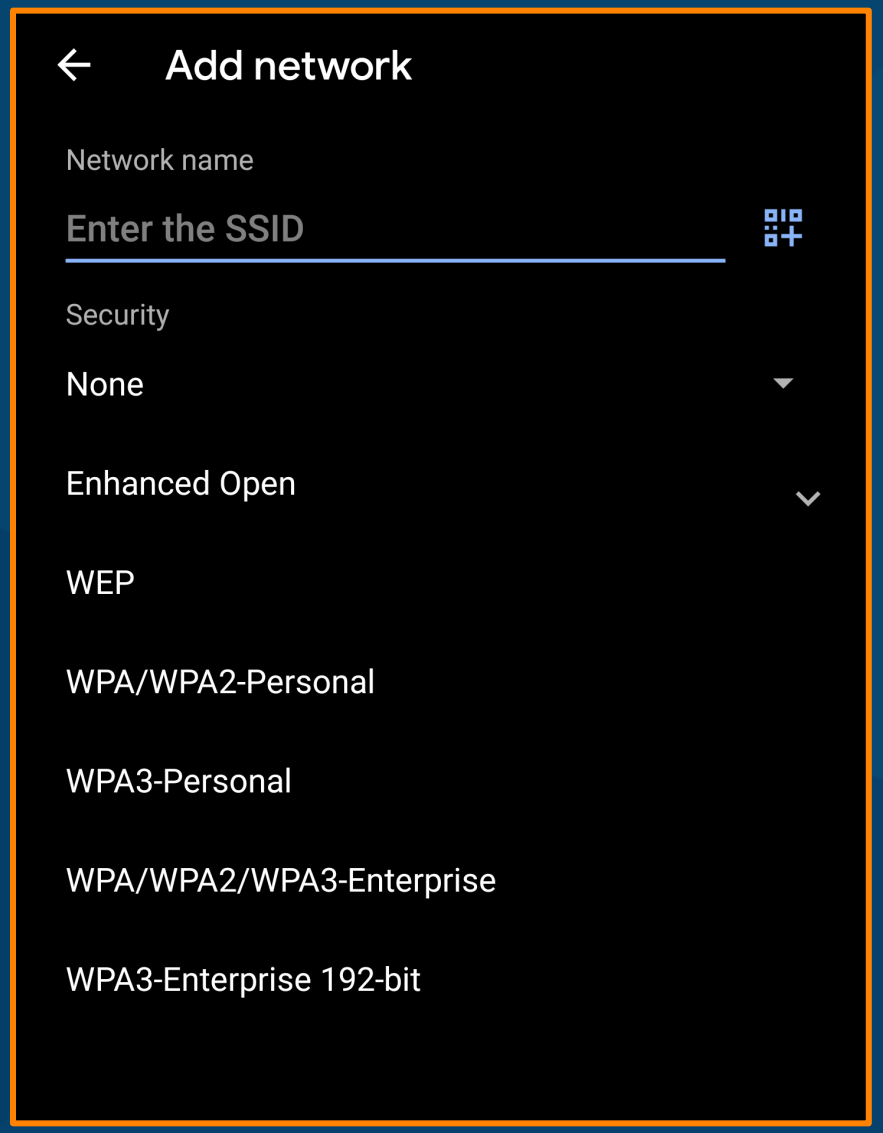
Tim Cappalli | Identity Architect @ Aruba

6/20/19

@ArubaNetworks

New Technologies

WPA3 and Enhanced Open



aruba
a Hewlett Packard Enterprise company

WPA3-Personal (SAE)

THE TECH	WHAT IT MEANS	UX IMPACT
Based off a Dragonfly key exchange	"Weak" passwords are less prone to to attack	None!
Zero knowledge proof	One passphrase guess per attack	

WPA3-Enterprise 192-bit Mode (CNSA)

THE TECH

192-bit encryption (Suite B)

TLS 1.2+

Restricted cipher suites

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
```

WHAT IT MEANS

EAP-TLS Only

Higher security

Not backwards compatible

EAP server certificate changes (3072-bit+ | P-384)

UX IMPACT

Not something an average end-user would need to configure

Enhanced Open

THE TECH	WHAT IT MEANS	UX IMPACT
Uses OWE (Opportunistic Wireless Encryption)	Datapath encryption by default!	Very little
Diffie-Hellman Key Exchange	Backwards compatible with legacy open	Potential new indicators

OS / Supplicant	WPA3				Enhanced Open (OWE)
	Personal	Personal with Password ID	Enterprise	Enterprise 192-bit Mode (CNSA)	
Windows 10	1903*				
Android	Q (10)*		Q (10)	Q (10)	Q (10)*
macOS	10.15				
iOS	13				
wpa_supplicant	2.7	2.7	2.7	2.7	2.7

iOS and macOS

Profile Installation Changes in iOS

Certificate Requirements
(macOS 10.15)

GENERAL

2048-bit or greater private key

SHA-256+ hash

Max 825 Days (leaf)

EAP SERVER CERTIFICATE

SAN must be present

Non-EV
(DV or OV)

Windows 10

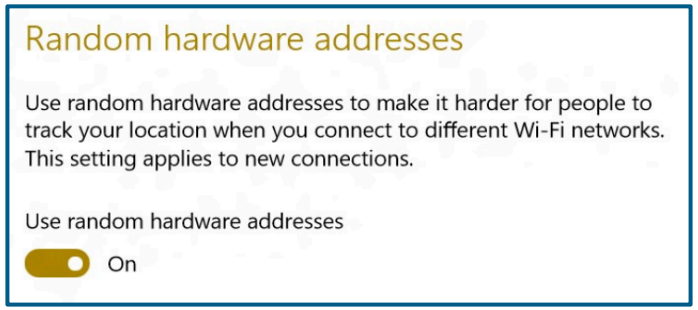
MAC Randomization in Windows 10

GLOBAL

Probe MAC randomized

MAC generated per saved ESSID

`Hash(MAC, secret, ESSID, connection ID)`

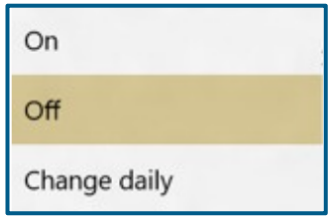


PER-ESSID

A. Use hardware MAC address

B. Use fixed random MAC address

C. Rotate MAC address daily



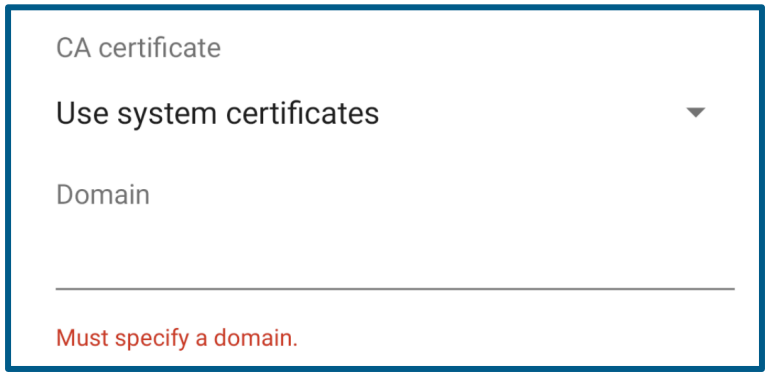
*** BOTH REQUIRE HARDWARE (AND DRIVER) SUPPORT ***

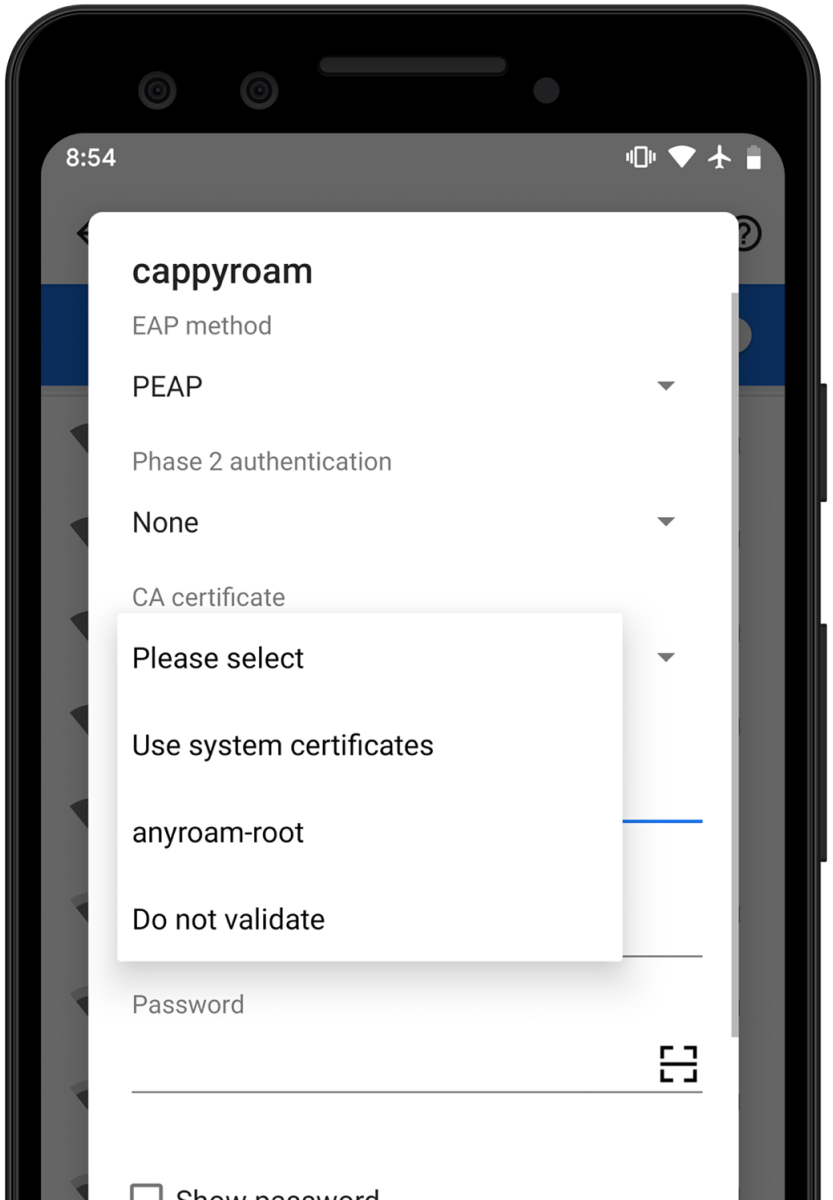
SOURCE: MICROSOFT

Android

EAP Server Certificate Validation

EAP server identity
validation must now be configured

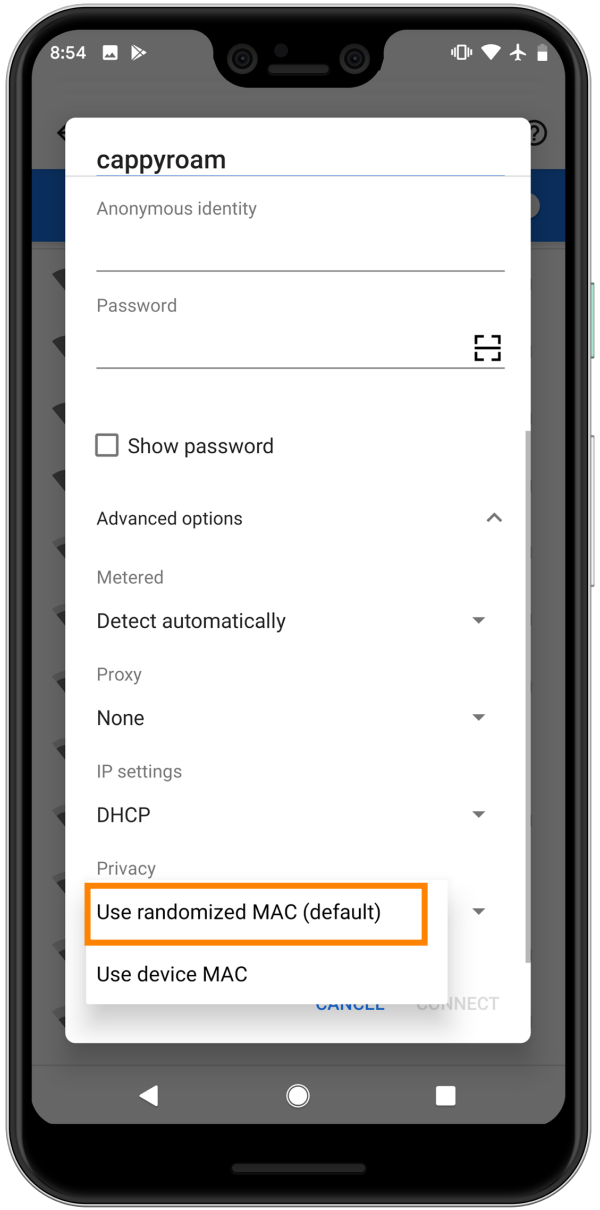




aruba
a Hewlett Packard
Enterprise company

MAC Randomization in Android

Android
Q



Enabled by default

Generated when the SSID is Saved to the network list

Persistent for OS instance lifetime

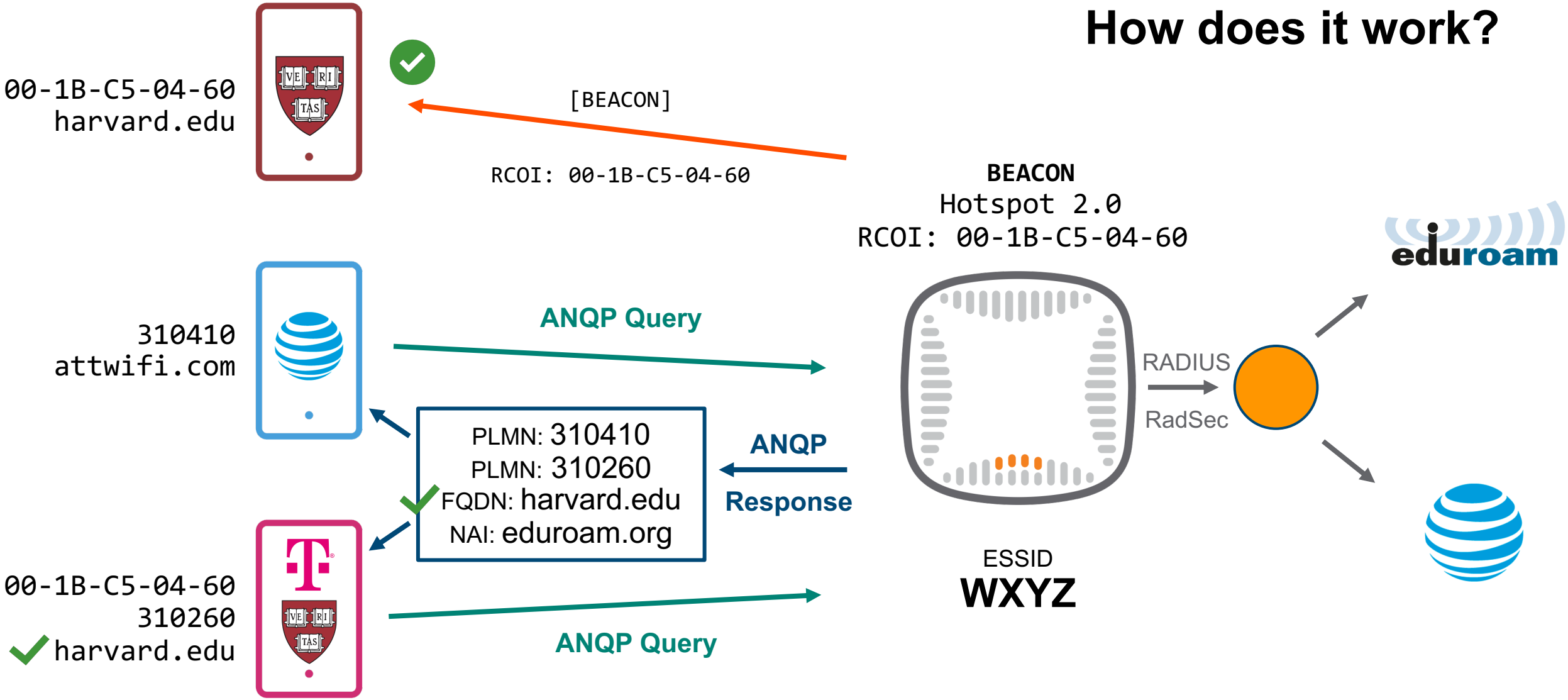
Manual control available

aruba
a Hewlett Packard Enterprise company

Passpoint

Hotspot 2.0

How does it work?



OS	R1	R2				R3
		OSU	EAP-TLS	EAP-TTLS	Remediation	
Windows 10						
Android		Q (10)	Q (10)	Q (10)	Q (10)	
macOS	*					
iOS	*					
wpa_supplicant						

aruba
a Hewlett Packard Enterprise company

Current Challenges

– Android EAP server trust

– iOS network selection behavior

– Apple's proprietary configuration format

– Windows 10 provisioning

– Privacy

RADIUS/TLS

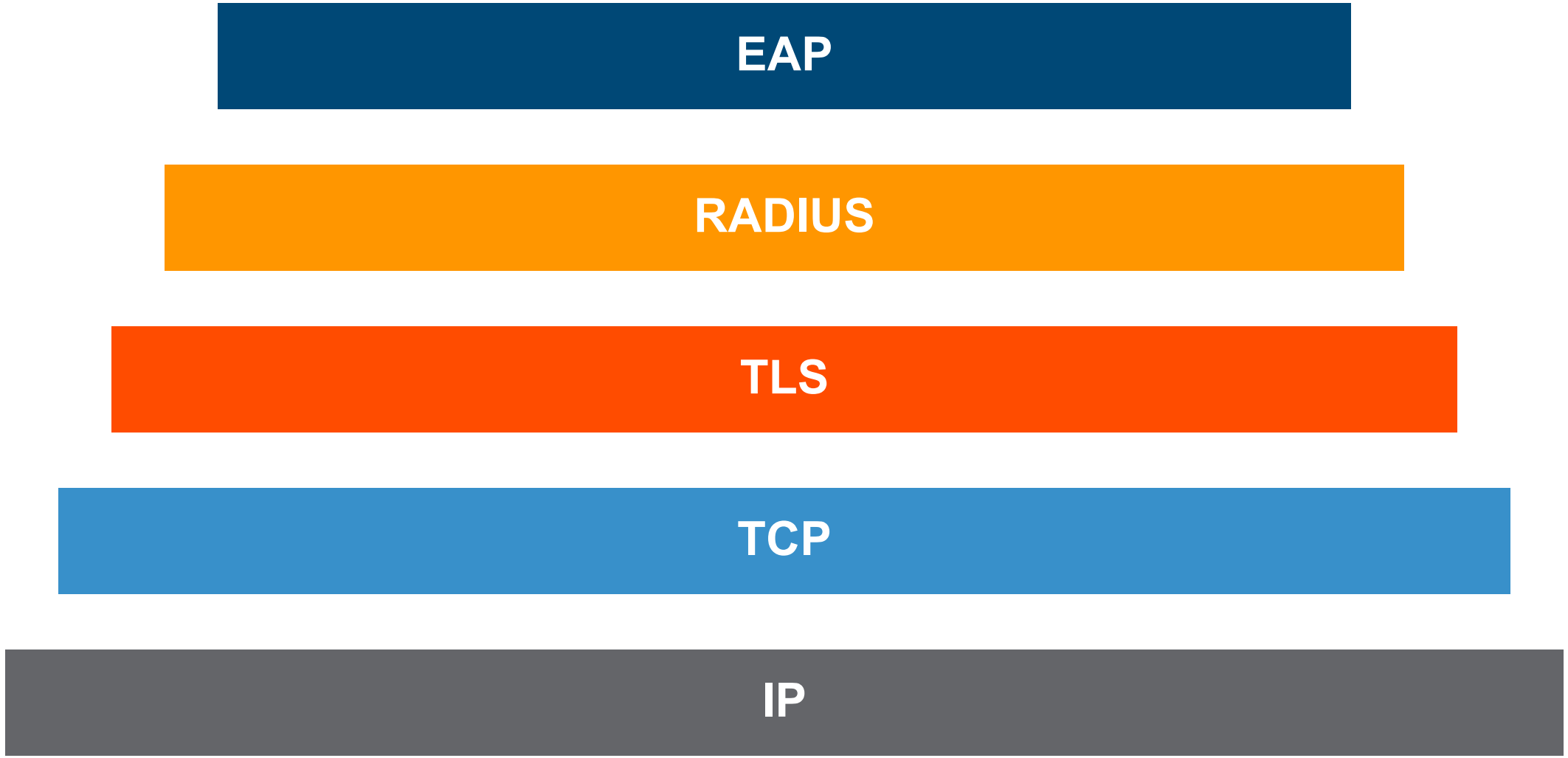
RadSec

RadSec Flavors

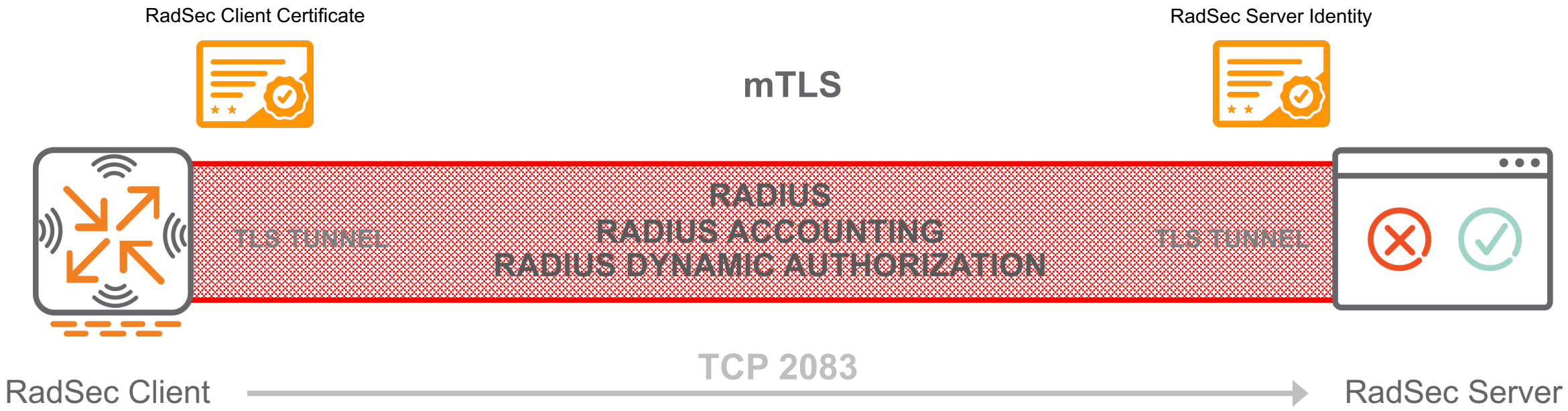
- RADIUS over TLS
  - Also referred to as RADIUS/TLS
  - TCP 2083

- RADIUS over DTLS
  - Also referred to as RADIUS/DTLS
  - UDP 2083

"EAP Stack" for RADIUS/TLS



RADIUS/TLS


RadSec Client Certificate
RadSec Server Identity
mTLS
TLS TUNNEL
RADIUS
RADIUS ACCOUNTING
RADIUS DYNAMIC AUTHORIZATION
TLS TUNNEL
TCP 2083
RadSec Client
RadSec Server

Why is RADIUS/TLS so important?

PERFORMANCE

Congestion control

No duplicate requests

Persistent session

No UDP fragmentation issues

SECURITY

(next few slides)

Why is RADIUS/TLS so important?

[Docs] [txt|pdf] [draft-ietf-nasr...] [Tracker] [Diff1] [Diff2]

Obsoleted by: 2138 PROPOSED STANDARD

Network Working Group
Request for Comments: 2058
Category: Standards Track

C. Rigney
Livingston
A. Rubens
Merit
W. Simpson
Daydreamer
S. Willens
Livingston
January 1997

Remote Authentication Dial In User Service (RADIUS)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

Table of Contents

Why is RADIUS/TLS so important?

```
▶ User Datagram Protocol, Src Port: 1812, Dst Port: 36918
▼ RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x93 (147)
    Length: 250
    Authenticator: 72d6262108a87b241a242183b19eccd4
    [This is a response to a request in frame 20744]
    [Time from request: 0.033581000 seconds]
  ▼ Attribute Value Pairs
    ▼ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
        Type: 26
        Length: 58
        Vendor ID: Microsoft (311)
      ▶ VSA: t=MS-MPPE-Recv-Key(17) l=52 val=c8e90f13fdf59aee1ab1b16f1dc1cc5a9057e922ce473ffa...
    ▼ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
        Type: 26
        Length: 58
        Vendor ID: Microsoft (311)
      ▶ VSA: t=MS-MPPE-Send-Key(16) l=52 val=d1b65014ea21cddb4155c84ec425b12471e6ac33318da373...
    ▶ AVP: t=EAP-Message(79) l=6 Last Segment[1]
    ▶ AVP: t=Message-Authenticator(80) l=18 val=e4915b66043edc0495e0c13f9e73efd2
    ▶ AVP: t=User-Name(1) l=10 val=mlavelle
    ▶ AVP: t=Vendor-Specific(26) l=22 vnd=Aruba Networks Inc(14823)
    ▼ AVP: t=Class(25) l=58 val=e885ee10bf3a420b9cd2e4706a53ea88100c000000000000...
        Type: 25
```

Why is RADIUS/TLS so important?

```
[The response to this request is in frame 4670]
▼ Attribute Value Pairs
  ▼ AVP: t=User-Name(1) l=35 val=asa-sensor.device.arubaboston.com
      Type: 1
      Length: 35
      User-Name: asa-sensor.device.arubaboston.com
  ▶ AVP: t=NAS-IP-Address(4) l=6 val=100.66.1.101
  ▶ AVP: t=NAS-Port(5) l=6 val=0
  ▶ AVP: t=NAS-Identifier(32) l=12 val=BOS-7010-A
  ▶ AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
  ▼ AVP: t=Calling-Station-Id(31) l=19 val=20-4C-03-31-20-8D
      Type: 31
      Length: 19
      Calling-Station-Id: 20-4C-03-31-20-8D
  ▶ AVP: t=Called-Station-Id(30) l=29 val=00-0B-86-9A-E3-D7:cappyroam
  ▶ AVP: t=Service-Type(6) l=6 val=Framed(2)
  ▶ AVP: t=Framed-MTU(12) l=6 val=1100
  ▶ AVP: t=EAP-Message(79) l=40 Last Segment[1]
  ▼ AVP: t=Vendor-Specific(26) l=17 vnd=Aruba Networks Inc(14823)
      Type: 26
      Length: 17
      Vendor ID: Aruba Networks Inc (14823)
    ▶ VSA: t=Aruba-Essid-Name(5) l=11 val=cappyroam
  ▼ AVP: t=Vendor-Specific(26) l=18 vnd=Aruba Networks Inc(14823)
      Type: 26
      Length: 18
      Vendor ID: Aruba Networks Inc (14823)
    ▶ VSA: t=Aruba-Location-Id(6) l=12 val=BOS-335-LR
  ▼ AVP: t=Vendor-Specific(26) l=16 vnd=Aruba Networks Inc(14823)
      Type: 26
      Length: 16
      Vendor ID: Aruba Networks Inc (14823)
    ▶ VSA: t=Aruba-AP-Group(10) l=10 val=BOS-Main
  ▶ AVP: t=Acct-Session-Id(44) l=29 val=204C0331208D-5C62D97D-1DC0E
  ▶ AVP: t=Message-Authenticator(80) l=18 val=4d8e048d0be85c23e68aec35a46eb96d
```

RADIUS/TLS Support

AEROHIVE NETWORKS

HiveManager*

Access Points

JUNIPER NETWORKS Mist AI is in the AIR™

Access Points

aruba

Mobility Controllers

Instant APs

Switches

ClearPass (6.8)

CISCO

Catalyst 9300
(as of 16.10)

Radiator

FreeRADIUS (v3) | Packetfence

aruba
a Hewlett Packard Enterprise company

Thanks!

Questions?

@ArubaNetworks