

Things are about to change

herrnilsson@sUNET.se

and

@halgefi

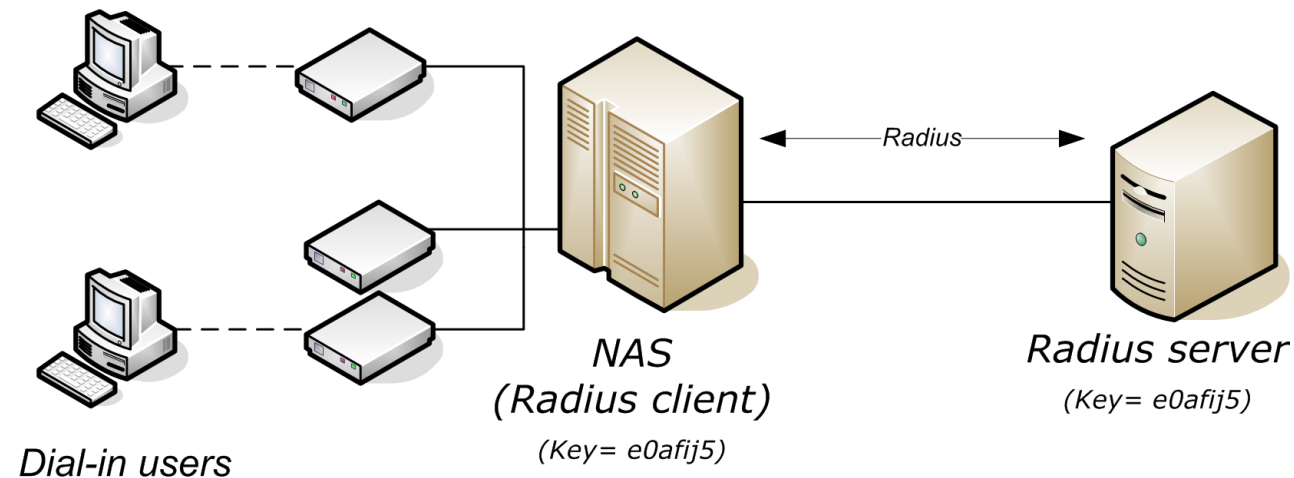


WHAT'S RADIUS???

Quoting <https://en.wikipedia.org/wiki/RADIUS>

RADIUS (Remote Authentication Dial-In User Services) is an **AAA** (authentication, authorization, and accounting) protocol that manages network access. RADIUS uses two types of **packets** to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. **Authentication** and **authorization** are defined in RFC 2865 while **accounting** is described by RFC 2866.

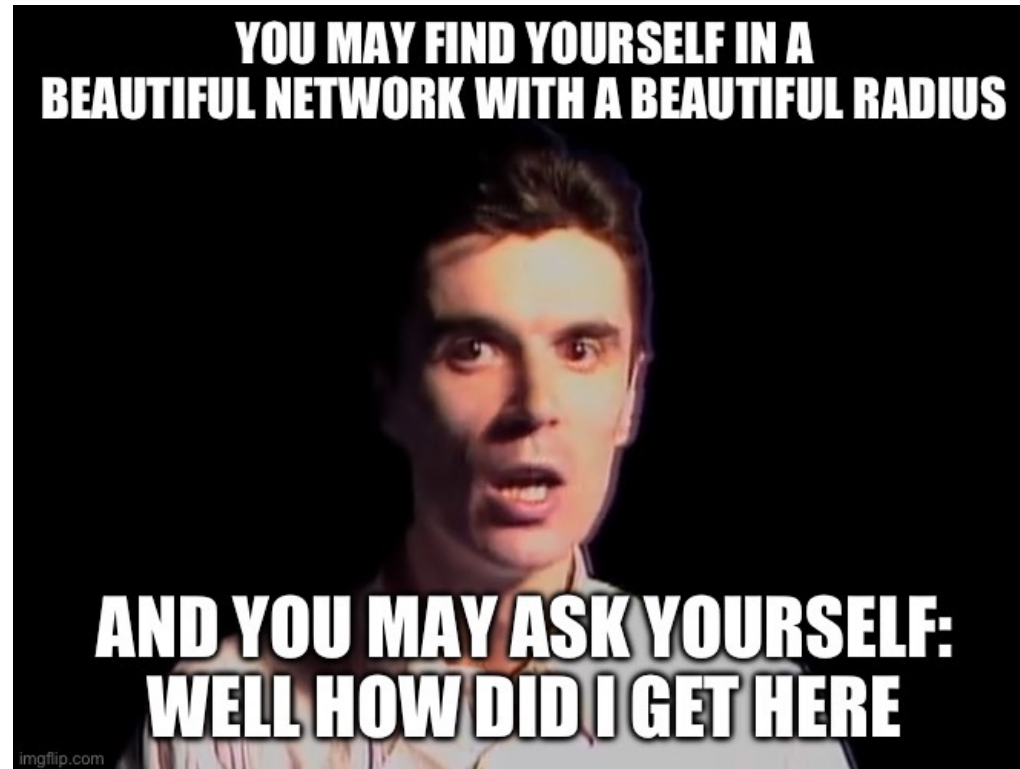
In the old days used in Modem Pools today mostly used for 802.1X and VPN



RADIUS???

RADIUS have now been around for 30 years and some of the basic mechanisms are still the same.

So is this a problem?



RADIUS getting old???

Quoting Alan Dekok (Freeradius) from TNC23:

What is wrong with RADIUS

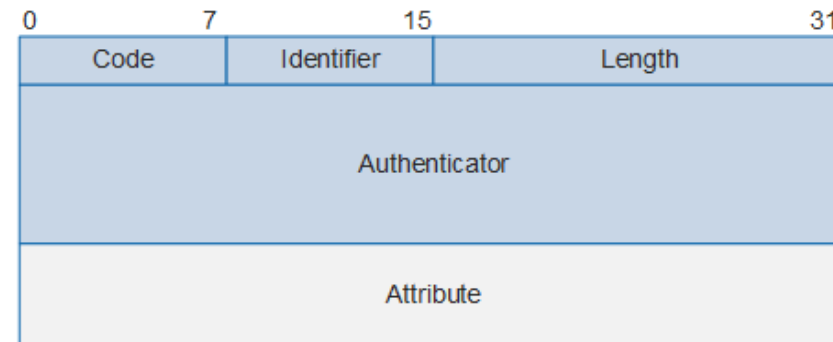


RADIUS is a dumpster fire of bad implementations and terrible security

- MD5 has been broken for a decade
 - <https://datatracker.ietf.org/doc/draft-dekok-radext-deprecating-radius/>
 - a hobbyist attacker can crack all possible RADIUS shared secrets of eight characters in about a day
- Users location can be tracked within 15m or less
- GPDR issues are large.

Why is it getting important to fix RADIUS?

- Today RADIUS is being used outside of the local network (eduroam, OpenRoaming, RADIUS in the Cloud)
- Old RADIUS is UDP based
- RADIUS unsecure, unencrypted with only a MD5 based Authenticator for the shared secret.
MD5 broken (RFC 6151)
<https://networkradius.com/articles/2022/10/04/radius-insecurity.html>
- Because the EAP packets riding embedded inside the RADIUS packets tunneled in TLS eduroam have been regarded as “safe” but having the whole RADIUS packet encrypted.



Timeline RADIUS (Greatest hits)

<https://datatracker.ietf.org/wg/radext/history/>

- 1991 Developed by Livingston Enterprises mainly for modem pools
- 2003 DIAMETER was developed as a better (twice as good as RADIUS 😊) replacement but never took off in Networking and was instead adopted by the mobility industry.
IETF WG DIME <https://datatracker.ietf.org/wg/dime/>
- 2004 IETF WG RADEXT begins their work in.
- 2006 A more standardized RADIUS emerges (much work done by eduroam community)
- 2012 RADSEC, Dynamic discovery, and RADIUS over TCP as draft
- 2014 Stefan Winter GÉANT/eduroam chairing the WG RADEXT making sure RADSEC and Dynamic Discovery becomes RFC:s
- 2023 Draft RADIUS 1.1 (now renamed to RADIUS ALPN to Remove MD5 Dependency)
ALPN = Application-Layer Protocol Negotiation Extensions and work for TLS 1.2 and above.
and upcoming RFC recommending not using old RADIUS standard other than locally.
(D)TLS based RADIUS with both PKI authentication and PSK mandatory on the server side.

Passpoint + RADSEC + Dynamic peer discovery = OpenRoaming



- Combining the following and you basically get OpenRoaming:
 - Wi-Fi Alliance Passpoint (based on 802.11u)
 - RADSEC RFC 6614 (RADIUS over TLS)
 - Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS
Based on the Network Access Identifier (NAI) RFC7585

New standards being developed:

(IETF work group RADEXT) <https://datatracker.ietf.org/wg/radext/about/>

- Moving RADIUS/TLS and RADIUS/DTLS to “standards track”
[draft-ietf-radext-radiusdtls-bis-00](#)
- FIPS compatible RADIUS: “RADIUS 1.1” [draft-ietf-radext-radiusv11-02](#)
<https://networkradius.com/articles/2023/05/25/introducing-radius-1-1.html>
 - How to keep your security people happy!
 - Will include 32-bit extended ID support
- CoA even when using NAT [draft-dekok-radext-reverse-coa-01](#)
- TLS-PSK (Workaround for those who don't love PKI 100%) [draft-ietf-radext-tls-psk-03](#)
- Multi-hop ping / traceroute packet (Get information about proxies!)

And finally

- Draft on mandating the end of using current UDP based RADIUS unless just doing it locally [draft-dekok-radext-deprecating-radius-05](#)

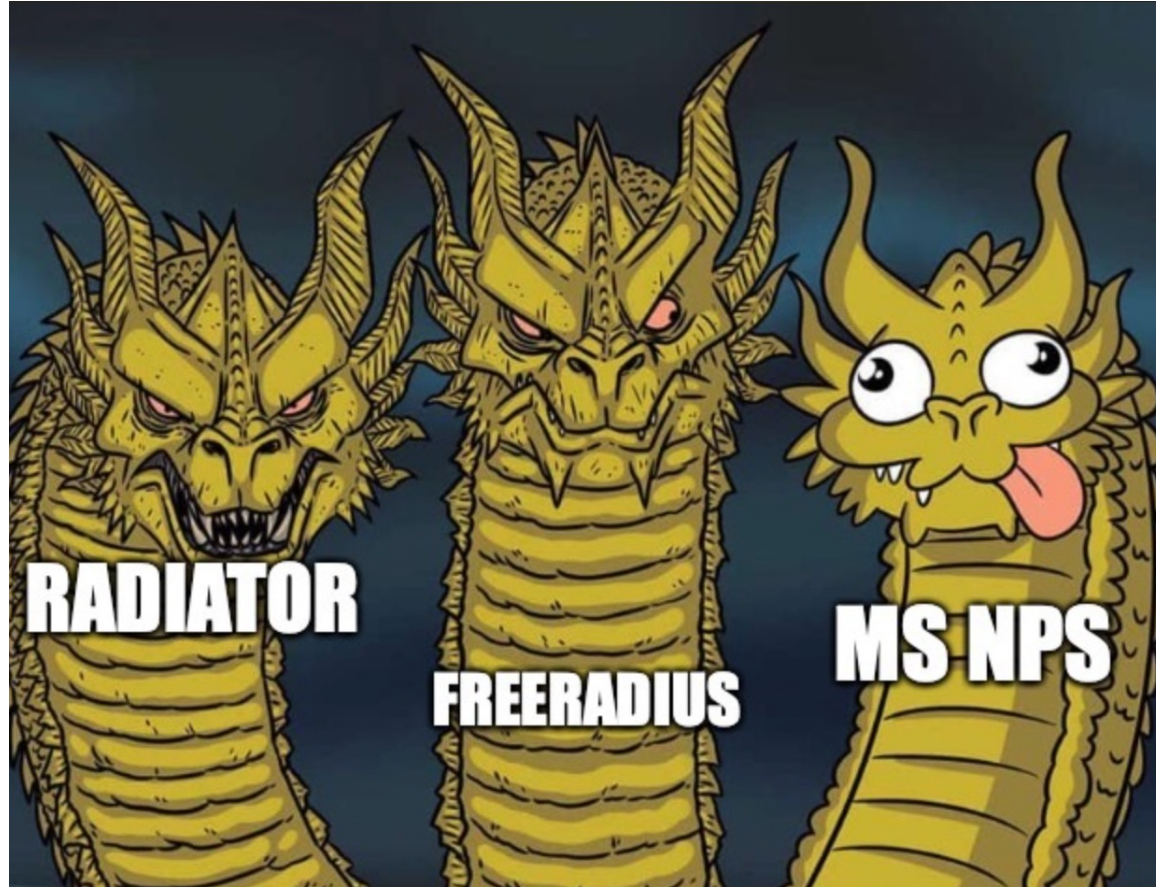
Feature Matrix of most used RADIUS servers

(Please let me know if something is wrong)

RADIUS NAS feature matrix still a work in progress

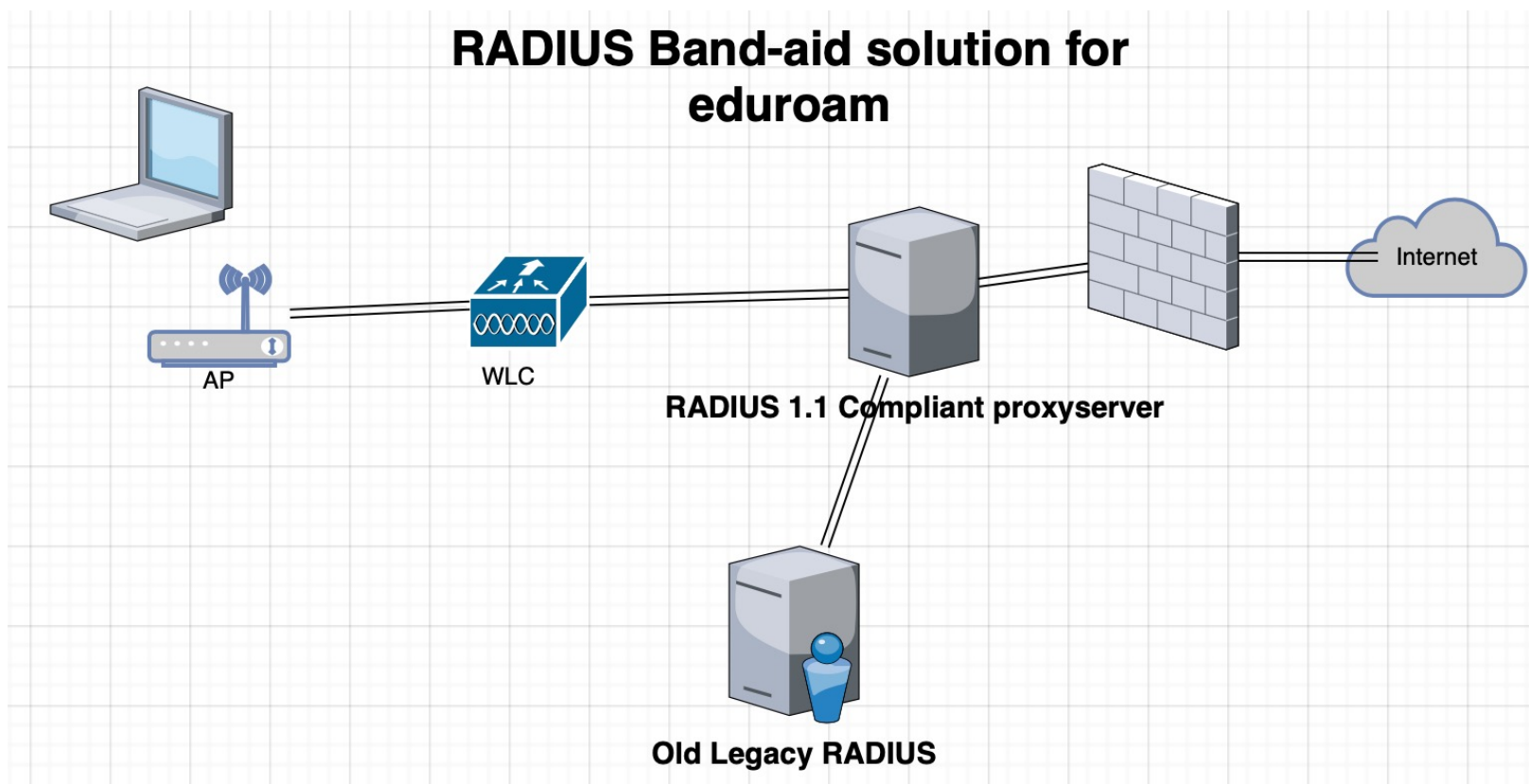
	Full RADSEC proxy support and dynamic discovery	RADIUS over (D)TLS	Attribute filtering	Server status	RADIUS 1.1	RADIUS TLS/PSK
FreeRadius (3.2.3)	YES	YES	YES (Whitelist)	Ja	Ja	Ja
Radiator	YES	ROADMAP	YES	Ja	ROADMAP	ROADMAP
NPS	NO	NO	NO	NO	NO	NO
Cisco ISE	NO	DTLS only ☹️	YES	NO?	NO	NO
Arista AGNI	NO	YES	UNKNOWN	UNKNOWN	NO	NO (Roadmap?)
Aruba Clearpass	UNKNOWN	YES	Ja (not verified)	YES?	NO	NO (Roadmap?)
RADSEC-Proxy	YES	YES	Ja (Whitelist)	Ja	Kanske???	YES (1.10)
MIST Access Assurance	UNKNOWN	YES?	???	UNKNOWN	NO	NO (Roadmap?)

Feature Matrix of RADIUS server's kind of indicates that some of us have problems.
Please try to keep up the pressure on the manufacturers.

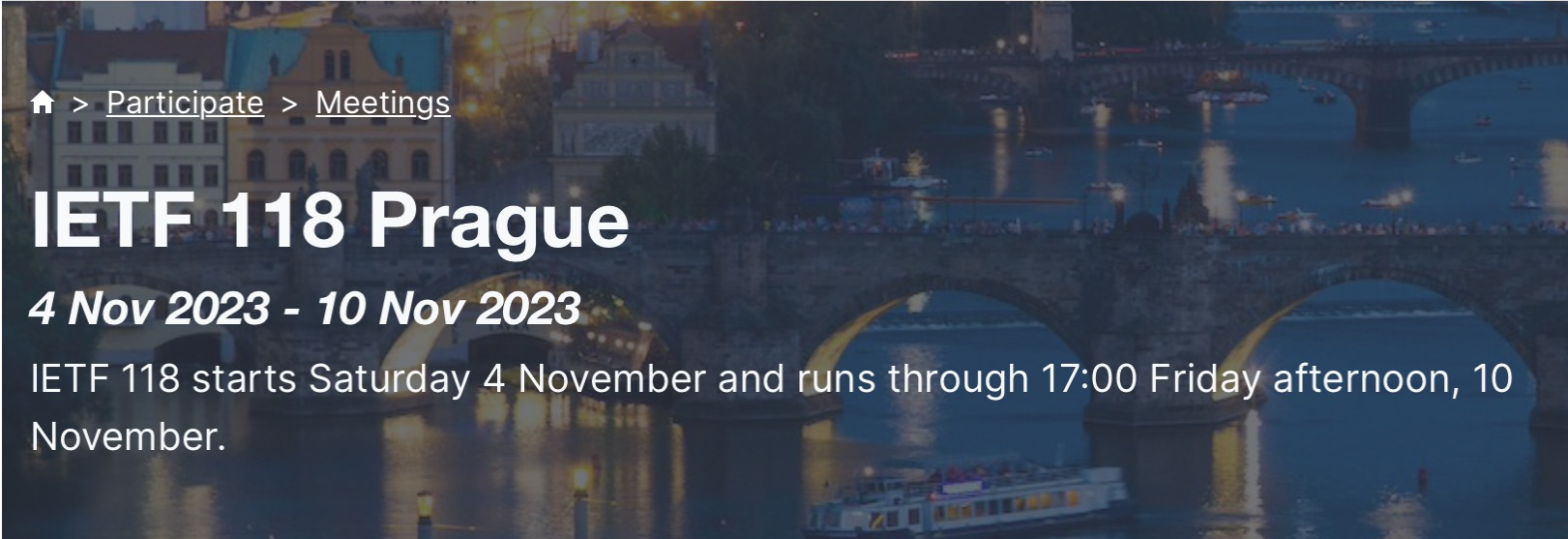


MS NPS, a groving pain

- Has been around for almost 8 years now without any major development
- Ongoing work within GÉANT on porting RADSECPProxy to Windows (GEANT development roadmap 2024)
- Start planning what to do when everything is Azure AD and Microsoft have retired NTLM.
- How many are still on NPS just because "We only do Microsoft here"?



- Want to stay up to date?
- IETF 118 happening here in Prague a week from now.
www.ietf.org

A banner for the IETF 118 Prague meeting. The background is a night view of the Prague skyline with the Charles Bridge and a boat on the river. The text is overlaid on the left side.

🏠 > [Participate](#) > [Meetings](#)

IETF 118 Prague

4 Nov 2023 - 10 Nov 2023

IETF 118 starts Saturday 4 November and runs through 17:00 Friday afternoon, 10 November.

RFC/Link Bonanza:



- <https://datatracker.ietf.org/wg/radext/about/>
- <https://radsecproxy.github.io>
- <https://networkradius.com/technology/news/>
- <https://en.wikipedia.org/wiki/RadSec>
- <https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/task/radsec-configuring.html>
- [https://documentation.meraki.com/MR/Encryption and Authentication/MR RADSec](https://documentation.meraki.com/MR/Encryption_and_Authentication/MR_RADSec)
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/sec/b_176_sec_9500_cg/configuring_radsec.pdf
- <https://files.radiatorsoftware.com/radiator/whitepapers/radsec-whitepaper.pdf>
- https://freeradius.org/documentation/freeradius-server/3.2.4/howto/protocols/proxy/enable_radsec.html
- <https://www.mist.com/documentation/radsec/>
- <https://www.mist.com/documentation/radsec/>
- <https://arista.my.site.com/AristaCommunity/s/article/AGNI-RadSec-Setup-using-AGNI-s-Internal-PKI>

Now RADIUS and this presentation have come full circle.
Thank you for listening.

Who was the builder of King
Arthurs round table?

Go on...

Sir Cumference.



THE END (or the beginning of the next Cycle?)

