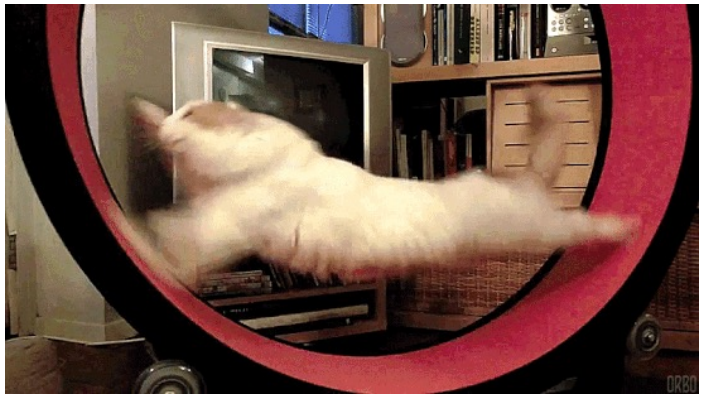
RADIUS och eduroam
(vill du gå framåt, gå i cirkel)

Nytt om det nyaste runt RADIUS och eduroam av Herr Nilsson



herrnilsson@sunet.se

SUNET

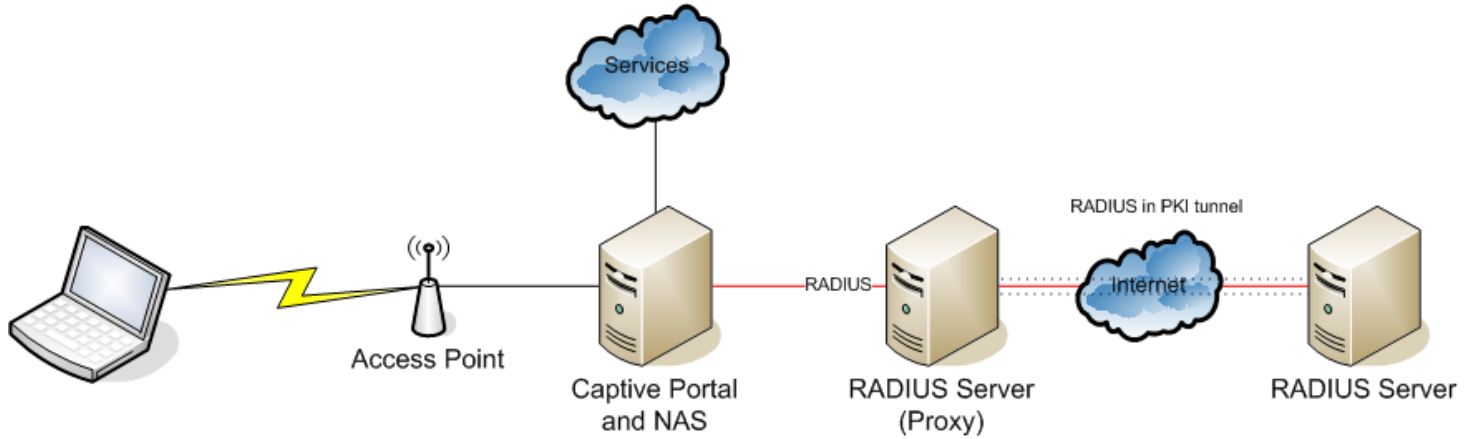
Bakgrund, hur fungerar RADIUS protokollet idag (speciellt ur ett eduroam-perspektiv)

- RADIUS (Remote Authentication Dial In User Service) skapedes 1991 för att hantera inloggning i modempooler och kan väl idag mer eller mindre ses som en dinosaurie som byggts på med mer och mer funktionalitet

Klippt ur https://en.wikipedia.org/wiki/RADIUS

Protocol components

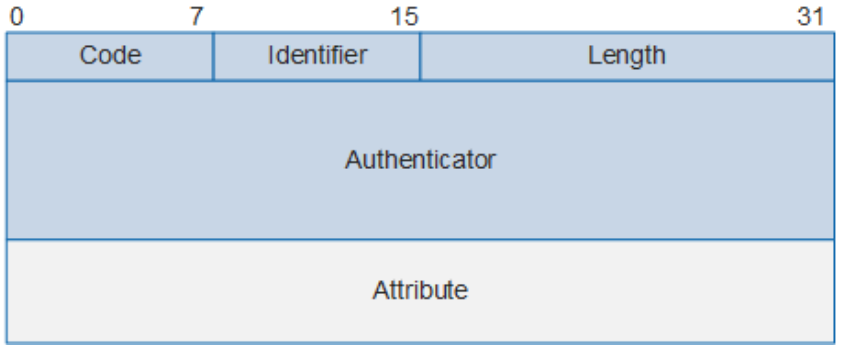
RADIUS is an AAA (authentication, authorization, and accounting) protocol that manages network access. RADIUS uses two types of packets to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. Authentication and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



SUNET

Bakgrund, hur fungerar RADIUS protokollet idag (speciellt ur ett eduroam-perspektiv)

- Diameter dök upp 2003 och var tilltänkt som en ersättare till RADIUS (2 gånger bättre 😉) men tyvärr tog det aldrig fart bland Nätverksfolket utan det fick bli Mobilindustrin som anammade.
  IETF WG DIME https://datatracker.ietf.org/wg/dime/about/
- RADIUS är i sin grundversion UDP baserat (problem med fyllda linor t.ex. SWEDAVIA i början med 100Mbit) RADIUS över TCP finns (RFC 6613) men används i praktiken inte i normalfallet.
- RADIUS är osäkert, Okrypterat med bara en MD5 Authenticator. MD5 knäckt (RFC 6151)
  https://networkradius.com/articles/2022/10/04/radius-insecurity.html
  Eftersom EAP packeten som åker ibäddade i RADIUS paketen varit tunnlade i TLS har eduroam ansetts som ”säkert”



- Detta ledde fram till jobbet med RADSEC 2012 (RFC 6614) men frågan var vilka stödde RADSEC tidigt?
  FreeRadius och Radiator var snabba upp på banan men en referensmjukvara saknades.
  Som en tillfällig och fortfarande fungerande ”nödlösning” RADSECProxy https://radsecproxy.github.io
- Fler som vill köra RADIUS i molnet: Hur få över RADIUS trafik säkert till molnet. Fler och fler NAS (Network Access Server) har börjat stödja RADSEC (inklusive ARISTA) men i dagsläget ingen med TLS/PSK
- AZURE AD och PEAP:s framtid (NTLM och MSCHAPv2 i framtiden). När ska NPS slutligen dö eller återuppstå?

SUNET

Tidslinje RADIUS historik (tänk er rösten av Hans Villius)
https://datatracker.ietf.org/wg/radext/history/

- 1991 Utvecklat av Livingston Enterprises för modempooler
- 2004 IETF Arbetsgruppen Gruppen RADEXT startar för att påbörja standardiseringsarbetet.
- 2006 Grunderna för en standariserad RADIUS fastställs
- 2012 RADSEC och RADIUS over TCP som draft
- 2014 Stefan Winter GÉANT/eduroam tar över klubban (Chair) för WG RADEXT och driver arbetet med RADSEC och Dynamic Discovery
- 2023 Stefan Winter slutar som ”Chair” men är fortfarande väldigt aktiv och en massa nyheter lanseras

SUNET

- Pågående IETF Arbete med att förbättra/förnya RADIUS standarden (work group radext) https://datatracker.ietf.org/wg/radext/about/

  - RADIUS 1.1 draft-ietf-radext-radiusv11-02 En rejäl omstöpning av RADIUS med krypterad Trafik (implikationer på eduroam?) https://networkradius.com/articles/2023/05/25/introducing-radius-1-1.html
  - RADSEC TLS/PSK draft-ietf-radext-tls-psk-03 (En väg att slippa ett framtida PKI elände)
  - RADIUS med mer än 8-bitars ID (Extended ID) inkluderat i RADIUS 1.1
  - Kommande RFC säger att okrypterad RADIUS över UDP ska undvikas om inte det körs lokalt draft-dekok-radext-deprecating-radius-04
  - Men vilka RADIUS mjukisar kommer att stödja detta???

SUNET

	Fullt RADSEC proxystöd inkl dymanic discovery	RADIUS över TLS	Attributfiltrering	Server status	RADIUS 1.1	RADIUS TLS/PSK
FreeRadius (3.2.3)	Ja	Ja	Ja (Whitelist)	Ja	Ja	Ja
Radiator	Ja	Roadmap	Ja	Ja	Roadmap	Roadmap
NPS	Nej	Nej	Nej	Nej	Nej	Nej
Cisco ISE	Nej	NJA DTLS	Ja	Nej	Nej	Nej
Arista AGNI	???	Ja	???	???	Nej	Nej (Roadmap?)
Aruba Clearpass	???	Ja	Ja (ej verifierad)	???	Nej	Nej (Roadmap?)
RADSEC-Proxy	Ja	Ja	Ja (Whitelist)	Ja	Kanske???	Ja (1.10)
MIST access assurance	???	Ja?	???	???	Nej	Nej (Roadmap)

- NPS, ett ökande problem
  - NPS is a dumpster fire!!! (Citat Alan DeKok, FreeRadius skapare)
  - Ingen utveckling har skett de senaste 5 åren. Begränsningar i NPS (Matris + Lista??)
  - Pågående arbete med att göra RADSECProxy körbart i Windows (GEANT development roadmap 2024) som en ”plåsterlösning”.
  - Börja redan nu planera för hur ni ska agera när Miscrosoft eventuellt stänger av NTLM.
  - Hur många kör kvar på NPS för att ”Vi kör bara Windows här”?

ComputerSweden

BRANSCH WHITEPAPERS NYHETSBREV

SÄKERHET 2023-10-17 07:08

Microsoft fasar ut stödet för NTLM i Windows 11

Mikael Markander

I fortsättningen ligger allt fokus på ersättaren Kerberos.

9

SUNET

- FreeRadius, saker att fundera på
  - Hur många kör FreeRadius i förhållande till NPS mm?
  - När uppgraderade jag till senaste rekommenderade versionen av FreeRadius?
  - Sitter jag kvar i gammal (2.0 version) för att jag inte törs eller vet hur man gör?
  - Känner jag att jag behärskar FreeRadius eller behöver jag förkovra mig
  - Finns det någon därute som känner sig jätte trygg med FreeRadius och vara mentor eller är detta någon som man vill att SUNET ska organisera

- Framtida kommande krav/rekommendationer på RADIUS från eduroam-sidan
  - Senast 202X ska alla eduroam anslutna köra RADSEC med TLS/PSK som ett minimum.
  - Senast 202X ska inget lärosätes IdP i det fallet att lösenordsbased EAP (PEAP-MsCHAPv2, TTLS-PAP mm) nyttja samma lösenord för eduroam som i SWAMI:s SAML-federation.
  - Lärosäten rekommenderas att gå över till EAP-TLS för eduroam (Geteduroam TBD)
  - Inga krav på RADIUS 1.1 i dagsläget
  - Under 2024 ska SUNET en labmiljö för testning av RADIUS (RADSEC, TSL/PSK mm

Gå nu in på SUNET forum (grupp eduroam) och besvara mina frågor (ett svar per lärosäte tack 😉)

- Länklista:
  - https://datatracker.ietf.org/wg/radext/about/
  - https://radsecproxy.github.io

SUNET