

EAP och 802.1X

Love Hörnquist Åstrand
Stockholms universitet

Sammanfattning

- EAP
- 802.1x
- IETF och IEEE
- AAA

EAP

- Autentisera användare till nätverks-utrustning
- PPP
- Ethernet inloggning till switch/hub (.1x)
- Wavelan inloggning (.1x)
- IKE

Ext Auth Proto

- RFC 2284 - PPP Extensible Authentication Protocol (EAP)
- RFC 3748 - Extensible Authentication Protocol (EAP)

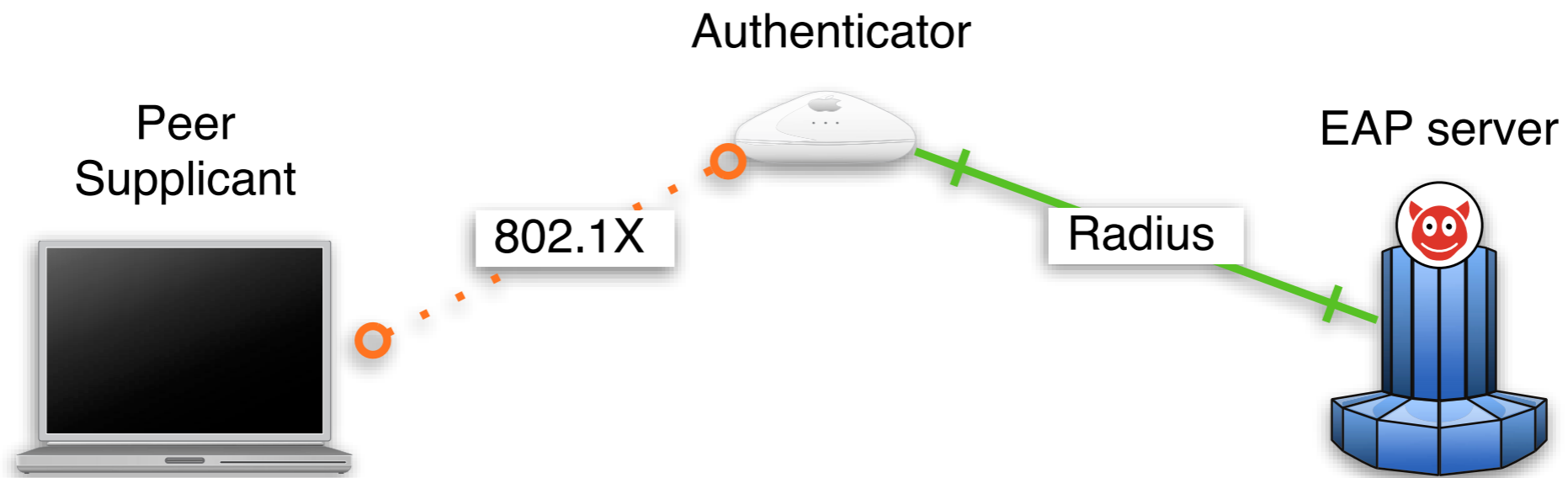
EAP Mekanismer

- Olika sätt att autentisera
- Lösenord , EAP-MD5, OTP, LEAP, EAP-FAST
- EAP-TLS, TTLS, PEAP
- EAP-SIM (GSM), EAP-AKA (UTMS)

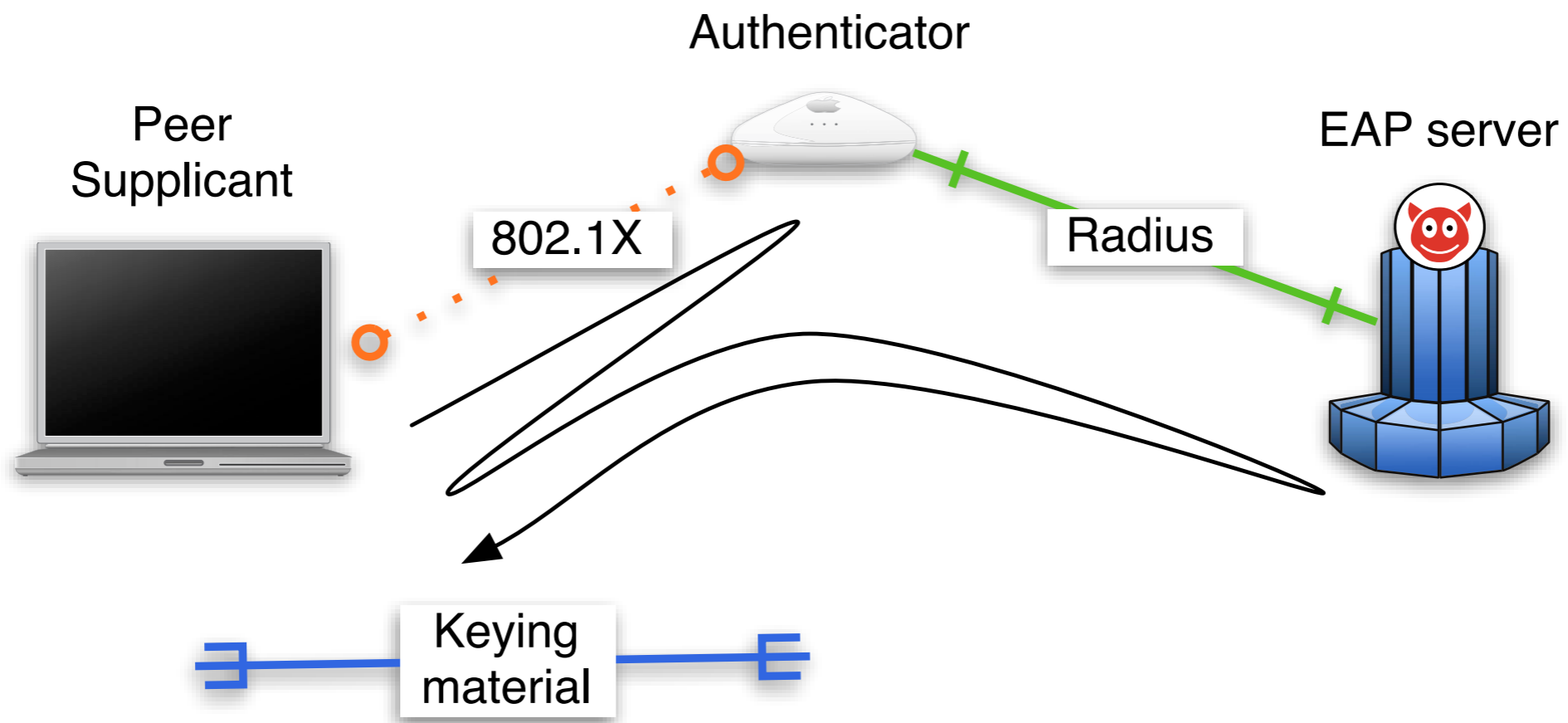
Spelare i EAP

- Authenticator (pass-through)
- backend authentication server
- EAP server
 - authenticator eller backend server
- Peer, Supplicant
- Mekanismer

Spelare i EAP, forts



EAP flöde



EAP packet

- 1. Request
- 2. Response
- 3. Success
- 4. Failure

EAP Request och Response typer

- 1. Identify
- 2. Notification
- 3. Nack
- 4 ... Mekanismer
- 254. Expanded Types
- 255. Experimental use

Identify

- Både som request och response
- Klienten kan frågar efter namn på utrustningen
- Svaret från nätutrustning kan innehålla mer info än bara vilka de är, peering partners

Network hints

- RFC 4282 - Network Access Identifier
 - DNS namn / Email liknade
 - Inte kompatibel med email/dns när man inte använder ASCII
- RFC 4284 - Roaming partners

Andra R&R packet

- Mekanism specifika

802.1X

- Ethernet (EAP Over Lan)
- 802.11-serien (wavelan)

EAP och 802.1X

- 802.1X transporterar EAP packet
- Definerar hur man pratar på länklager
- EAP ger nyckel-material till 802.1X och underliggnade länklager. WEP/WPA nycklar.

Ethernet

- Välkänd multicast adress

EAP over wavelan

- Basstationen som man associerade med

IETF vs IEEE

- 802.1x är en IEEE standard
- EAP är en IETF standard
- EAP mekanismer är IETFs “ansvar”

IETF EAP wg

- Jobbar på EAP protokollet
- Extensibility
- Network selection problem definition
- EAP state-machine
- EAP keying material

IETF EMU wg

EAP Method Update

- Skapades för att möta krav från andra SDOer
- 40 olika EAP metoder finns
- Många inte publicerade
- EAP-TLS
- Strong shared secrets
- Lösenord

AAA

- Radius
- Diameter

Radius

- Vanligast
- Använder MD5 för integritet
- Använder MD5 för kryptering av lösenord!
- Radius arbetsgruppen i IETF arbetar på problemet
- En del kör Radius över TLS

Diameter

- IETF djur
- Tänkt att ersätta Radius

Frågor
efter lunch