

# 802.1X & EAP & Keying

## 802.1 Status Update

Paul Congdon  
Hewlett Packard

# The Work Going On

- Several specifications MUST align to enable a working implementations:
  - IEEE 802.1aa (update to 802.1X)
    - <http://www.ieee802.org/1/files/private/aa-drafts/d5/>
    - <http://www-personal.umich.edu/~jrv/eap.htm>
  - IEEE 802.11 TG1 (security)
    - [http://www.ieee802.org/11/private/Draft\\_Standards/11i/802.11i-D3.0.doc](http://www.ieee802.org/11/private/Draft_Standards/11i/802.11i-D3.0.doc)
  - RFC 2284bis (EAP)
    - <http://www.levkowetz.com/pub/ietf/drafts/eap/>
    - <http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-01.txt>
    - <http://www.drizzle.com/~aboba/EAP/eapissues.html>
  - EAP state machine work
    - <http://www.ietf.org/internet-drafts/draft-ietf-eap-esteem-01.txt>
    - <http://www.ietf.org/internet-drafts/draft-vollbrecht-eap-state-01.txt>
  - RFC 2869bis (RADIUS support for EAP)
    - <http://www.drizzle.com/~aboba/EAP/draft-aboba-radius-rfc2869bis-10.txt>
  - Draft-congdon (RADIUS and 802.1X)
    - <http://www.ietf.org/internet-drafts/draft-congdon-radius-8021x-23.txt>

# What has been done so far?

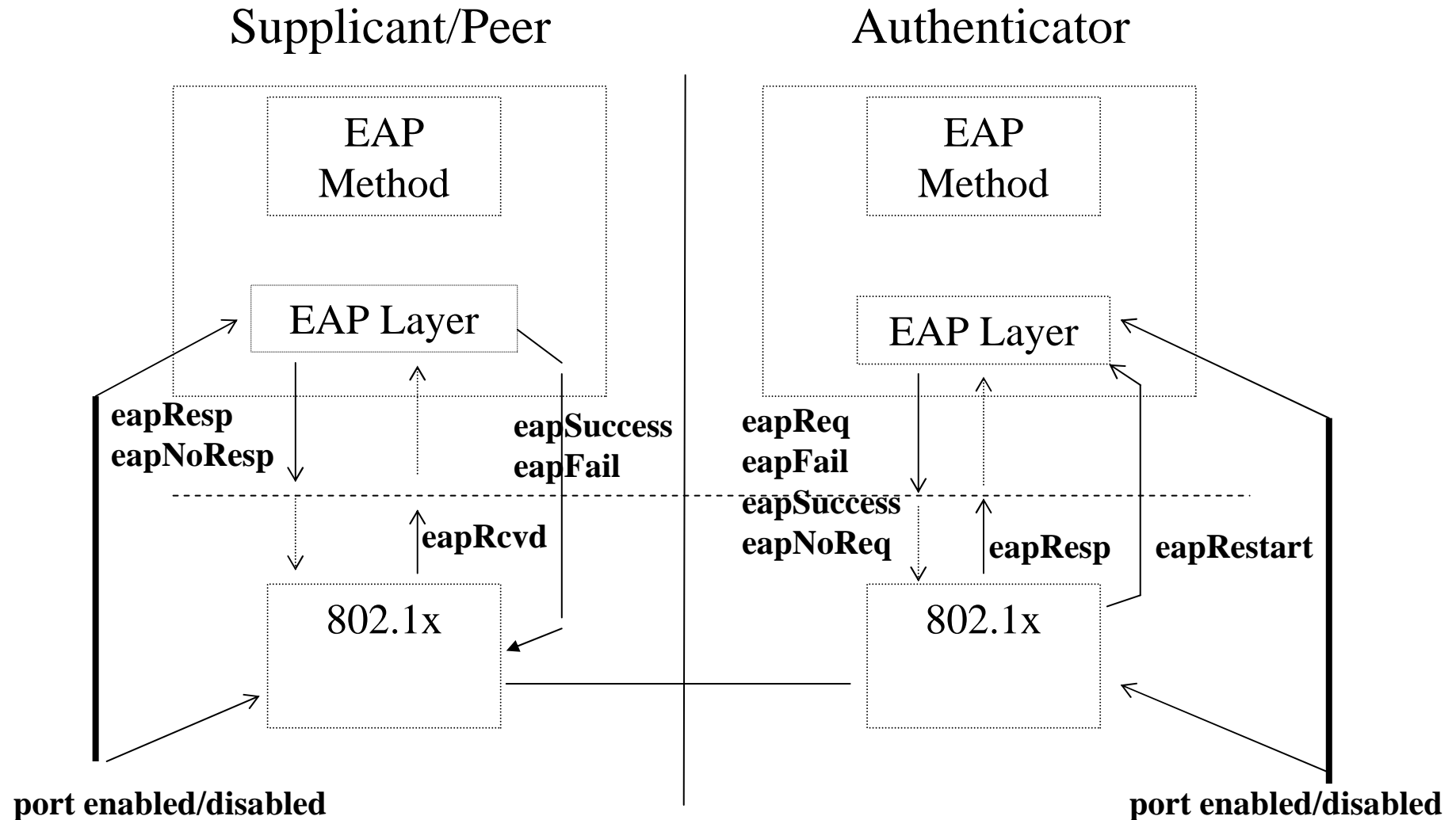
- A number of issues resolved with RFC 2284bis (EAP)
  - <http://www.drizzle.com/~aboba/EAP/eapissues.html>
- Interface between 802.1X and EAP well defined
  - <http://www-personal.umich.edu/~jrv/eap.htm>
- Preliminary EAP state machines defined
  - <http://www.cs.umd.edu/~npetroni/EAP/>
- Last call on RFC 2869bis (RADIUS/EAP)
  - <http://www.ietf.org/internet-drafts/draft-aboba-radius-rfc2869bis-09.txt>
- Last call on draft-congdon (RADIUS/802.1X)
  - <http://www.ietf.org/internet-drafts/draft-congdon-radius-8021x-23.txt>
- Proposed changes to 802.1X machines and 802.1aa/D5
  - <http://www-personal.umich.edu/~jrv/eap.htm>
- Proposed changes to key interface for 802.11i
  - <http://www-personal.umich.edu/~jrv/eap.htm>

# Proposed and Agreed Changes to 802.1aa/D5

- Specification of interface between EAP/802.1X
- No more EAP packet processing in 802.1X
- Addition of controlled port in Supplicant
- Initial Authenticator request comes from EAP not 802.1X
- Ability for EAP to silently discard frames
- Proposed inclusion of EAP machines in 802.1X Annex
  - **ISSUE:** How to coordinate this with ongoing work in IETF
- EAPOL-Key exchange sequenced before EAP-Success
- Propose update generic key machines to match a well defined interface within 802.1X. 802.11 TG<sub>i</sub> to use this interface for 4-way handshake.

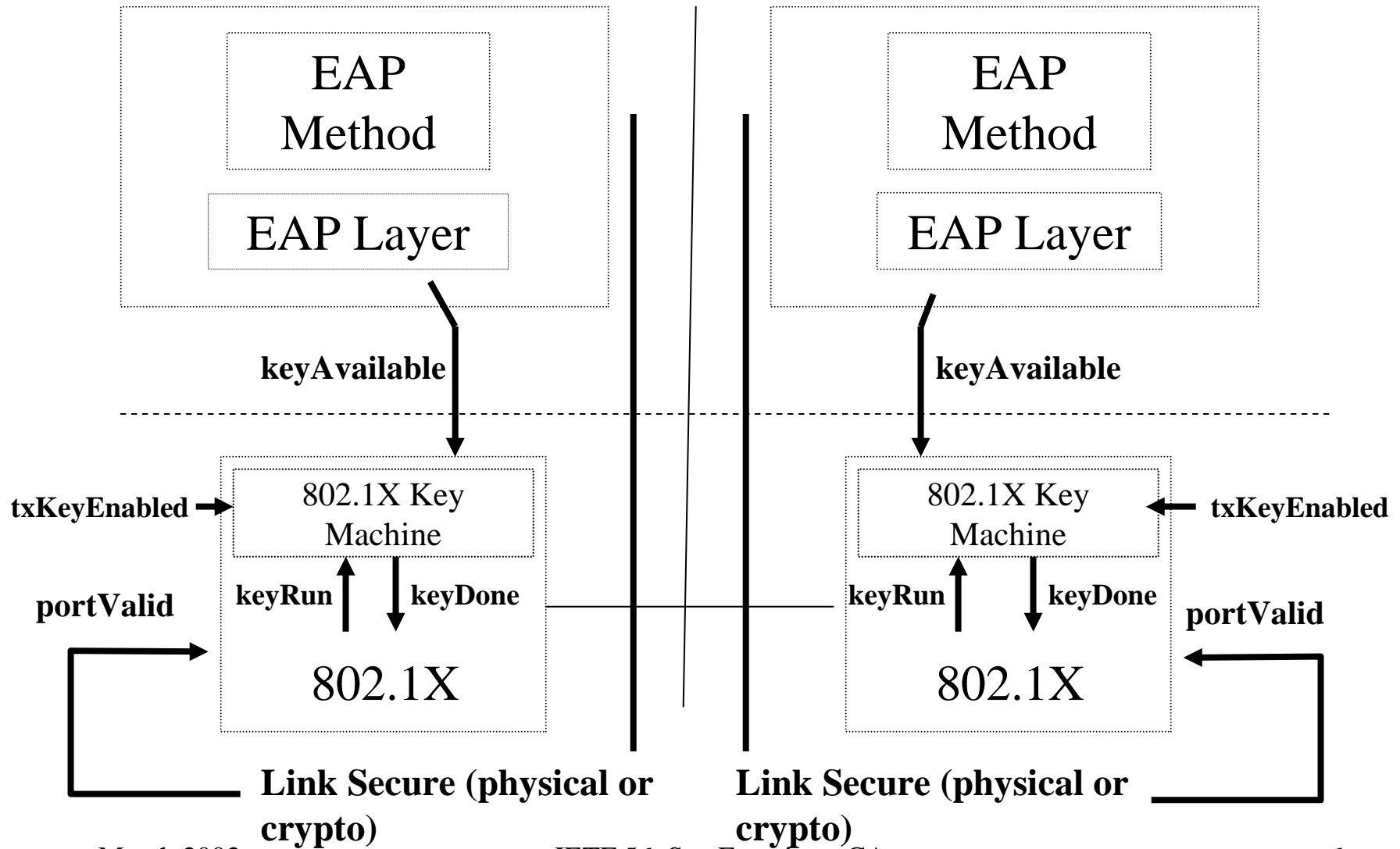
# EAP / 802.1X Interface

*(excluding key exchange)*



# Key Interface with EAP

## 802.1X & 802.11



# LinkSec Task Group Formation in 802.1

- Study group was formed to recommend work on a broad 802 security architecture
  - <http://www.ieee802.org/linksec/>
- Agreement to transform into a new Task Group within 802.1
- Likely to leverage and move forward 802.1X and 802.11 TGi models using EAP.